IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
GALVESTON DIVISION

BEVERLY T. PETERS, individually and on behalf of all others similarly situated, **PLAINTIFF** **v.** **ST. JOSEPH SERVICES CORP. d/b/a ST. JOSEPH HEALTH SYSTEM and ST. JOSEPH REGIONAL HEALTH CENTER,** **DEFENDANTS**	**CASE NO.: 3:14-cv-00114** **JURY TRIAL DEMANDED**

PLAINTIFF'S SURREPLY TO DEFENDANTS' PENDING MOTIONS

TO THE HONORABLE UNITED STATES DISTRICT COURT:

Plaintiff Beverly T. Peters ("Peters"), on behalf of herself and all others similarly situated, files this brief Surreply to the pending motions filed by Defendants St. Joseph Services Corporation d/b/a St. Joseph Health System and St. Joseph Regional Health Center (together, "St. Joseph") (Doc. ##s 23-27), and respectfully shows the following:

INTRODUCTION

St. Joseph's five-page Consolidated Reply (Doc. #39) is telling for what it does not address. It does not rebut—much less, address—Peters' response to St. Joseph's Rule 12(b)(1) motion to dismiss. It also does not rebut—much less, address—Peters' response to St. Joseph's motion to transfer venue. It also does not rebut—much less, address—Peters' response to St. Joseph's motion to strike. Nor does it rebut—much less, address—Peters' response to St. Joseph's motion to strike and/or deny class certification.

Rather, St. Joseph's Reply only addresses a small portion of Peters' response to its Rule 12(b)(6) motion to dismiss—the arguments pertaining to her two Fair Credit Reporting Act ("FCRA") counts and whether the Court should exercise supplemental jurisdiction over her state law claims should the FCRA counts be dismissed. St. Joseph, however, does not address the arguments pertaining to her other eleven (11) counts. *See* Complaint (Doc. #22, ¶¶ 82-146).

St. Joseph's limited Reply arguments are erroneous. Its Rule 12(b)(6) motion to dismiss Peters' FCRA claims, and its further request that the Court decline to exercise its supplemental jurisdiction if the FCRA claims are dismissed should be denied for the following additional reasons.

ARGUMENTS AND AUTHORITIES

A. Peters properly states claims for St. Joseph's FCRA violations (Counts I and II, Complaint, ¶¶ 66-81).

In its Reply, St. Joseph cites, for the first time, *Garnett v. Millenium Med. Mgm't Res., Inc.,* No. 10-C-3317, 2010 WL 5140055 (N.D. Ill. Dec. 9, 2010), *D'Angelo v. Wilmington Med. Ctr., Inc.*, 515 F.Supp. 1250 (D.De1. 1981), *Mitchell v. Surety Acceptance Corp.*, 838 F.Supp. 497 (D.Colo. 1993). *Id.* at 2. All of these cases were available at the time St. Joseph filed its motion to dismiss—but were not cited. It is now too late to assert new authority in its Reply that was not raised by Peters in her response. St. Joseph, therefore, has waived its right to assert *Garnett*, *D'Angelo*, and *Mitchell*. *See United States v. Whitfield*, 590 F.3d 325, 346 (5th Cir. 2009). Respectfully, the Court should disregard these cases.

Even then, *Garnett*, *D'Angelo*, and *Mitchell* do not provide a basis for dismissing Peters' FCRA counts. Each medical data breach case—including *Garnett*, *D'Angelo*, *Mitchell* and this case—has its own set of nuanced facts, which St. Joseph does not explore in its Reply. Sound bites from *Garnett*, *D'Angelo*, and *Mitchell*, none of which are Texas (or even Fifth Circuit) cases, cannot be blanketly argued as controlling precedent here.

Nor does St. Joseph provide a comparative analysis of the allegations in the *Garnett*, *D'Angelo*, and *Mitchell* complaints with the allegations in Peters'

Complaint. The *Garnett* complaint, in fact, suffers from conclusory pleading defects that do not exist here, to wit:

> *Plaintiffs repeat the statutory language in conclusorily* (sic) alleging that each defendant is a [consumer reporting agency (CRA)]. Compl. ¶ 32. … Plaintiffs must allege sufficient facts to plausibly support that each defendant is a CRA. (citation omitted). The *minimal allegations* regarding the nature of defendants' businesses do not plausibly support that either defendant regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. …
>
> The *minimal facts alleged by plaintiff* regarding activities of defendants provide support for concluding each defendant is not a CRA. Particularly in that light, *a conclusory allegation that each defendant is a CRA* is not sufficient to plausibly support that either defendant is a CRA.

2010 WL at *2 and *3 (emphasis added). Peters' FCRA allegations, on the other hand, are detailed and specific. *See* Complaint, ¶¶ 66-81 (especially ¶74 pertaining to Peters' "consumer reporting agency" allegations).

Moreover, the 20+ year old non-data breach summary judgment opinion in *D'Angelo* pertains to defendants Credit Bureau of Wilmington, Inc. and Credit Bureau Associates—not the Wilmington Medical Center, the alleged health care provider most closely analogous to St. Joseph. Similarly, *Mitchell*, a 20+ year old non-data breach summary judgment opinion, involved a consumer who sued a debt collection agency—not a health care provider. *D'Angelo* and *Mitchell* are inapposite to this case and do not apply.

St. Joseph also recycles *Willingham v. Global Payments, Inc.*, 1:12-CV-01157-RWS, 2013 WL 440702 (N.D. Ga. Feb. 5, 2013) and *Holmes v. Countrywide Fin. Corp.*, 5:08-CV-00205-R, 2012 WL 2873892 (W.D. Ky. July 12, 2012) on the "furnishing" issue. Reply at 2-3. Peters addressed this argument in her response (*id*. (Doc. #37) at 12-14), and will not repeat her arguments here.

The fact that St. Joseph repeatedly states Peters' FCRA allegations are conclusory does not make it so. In fact, the opposite is true. Her FCRA allegations are substantive and on point. Peters properly states claims for St. Joseph's FCRA violations; its Rule 12(b)(6) motion to dismiss should be denied.

B. Even if the Court dismisses Peters' FCRA claims, it should exercise supplemental jurisdiction over her remaining state law claims.

St. Joseph recycles its argument that the Court should decline to exercise supplemental jurisdiction over her state law claims should the FCRA claims be dismissed. Reply at 4-5. St. Joseph claims Peters fails to explain why the Court *should* exercise its supplemental jurisdictions in such a case. *Id*. Not true. Peters noted that the Parties' resources would be wasted if they had to start over in state court in light of the work that has been done to date in this Court. Response at 15.

St. Joseph offers no authority *requiring* dismissal of Peters' state law claims should her FCRA counts be dismissed and, in fact, admits the "Court most certainly has ***discretion*** to exercise supplemental jurisdiction over state law claims when no remaining federal claims exist." Reply at 4 (emphasis in original). More

important, St. Joseph fails to explain why the Court is not "suitable and capable of interpreting all remaining Texas and common law claims should the FCRA claims be dismissed." *Id*.

NOTICE OF ADDITIONAL AUTHORITY

Peters also alerts the Court to two recent data breach opinions that were issued prior to St. Joseph filing its Reply.

In *In re Adobe Systems, Inc. Privacy Litigation*, No. 13-CV-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014) (Exhibit A), plaintiffs assert various claims against Adobe arising out of a 2013 intrusion into Adobe's computer network and the resulting data breach. Plaintiffs alleged they have suffered at least one of three types of cognizable injuries-in-fact: (i) increased risk of future harm, (ii) cost to mitigate the risk of future harm and/or (iii) loss of the value of their Adobe products. *Id*. at *5.

Adobe sought to dismiss the case, asserting the same *Clapper* Article III standing arguments St. Joseph asserts here. The court rejected Adobe's arguments, holding that "*Clapper* did not change the law governing Article III standing" (*id*. at *7) and the threatened increased risk of harm was "sufficiently concrete and imminent to satisfy *Clapper*" (*id*. at *8) because:

> Unlike in *Clapper,* where respondents' claim that they would suffer future harm rested on a chain of events that was both "highly attenuated" and "highly speculative," 133 S.Ct. at 1148, *the risk that Plaintiffs' personal data will be misused by the hackers who breached*

> *Adobe's network is immediate and very real*. Plaintiffs allege that the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates. (citation omitted). Plaintiffs' personal information was among the information taken during the breach. (citation omitted). *Thus, in contrast to Clapper, where there was no evidence that any of respondents' communications either had been or would be monitored, … here is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken.* …
>
> Indeed, the threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused. However, to require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be "literally certain" in order to constitute injury-in-fact. *Clapper*, 133 S.Ct. at 1150 n. 5; *see also, e.g., Monsanto*, 561 U.S. at 153–54, 130 S.Ct. 2743 (finding that a "substantial risk of gene flow" from genetically engineered alfalfa crops to non-genetically engineered alfalfa crops was sufficient to confer Article III standing).

Id. at *8. The same is true here—especially in light of Peters' detailed narrative of her post-Data Breach experience. *See* Complaint (Doc #22), ¶¶ 11-19 (and accompanying notes).

In *Tierney v. Advocate Health and Hosp. Corp.*, No. 13-CV-6237 (N.D. Ill. Sept. 4, 2014) (Exhibit B),[1] a medical data breach class action in which plaintiffs allege FCRA counts, the court found Article III standing as to two plaintiffs because, similar to this case, they allege "one or more individuals attempted to

[1] Richard L. Coffman, one of Peters' counsel, is Co-Counsel for plaintiffs in *Tierney*.

access personal bank accounts and had opened cell phone accounts" and plaintiff Benkler "alleges that he has never been a victim of a data breach aside from Defendant's data breach." *Id*.

Nevertheless, and without performing any detailed legal analysis, and without any evidence before it, the court dismissed plaintiffs' FCRA claims, finding (i) the defendant was not a "consumer reporting agency" under FCRA, and (ii) plaintiffs failed to "plausibly allege that [d]efendant 'furnished' any information to a third party." *Id*.

With all due respect to the *Tierney* court, Peters asserts the case was decided incorrectly.[2] The "consumer reporting agency" issue is a fact issue. It was intellectually impossible for the court to conclude on a pre-discovery Rule 12(b)(6) motion—without any evidence before it—that defendant did not engage in conduct of the kind that qualified it as a FCRA "consumer reporting agency." *See* 15 U.S.C § 1681a(f).

Under the Rule 12(b)(6) standard of review, a court is required to accept the facts pled in the complaint as true. Here, Peters specifically alleges that St. Joseph engages in the 15 U.S.C § 1681a(f) "consumer reporting agency" activities "for the ultimate purposes of, *inter alia*, establishing [Peters'] and Class Members' eligibility for health care services, confirming whether such health care services

[2] The *Tierney* plaintiffs intend to appeal the court's decision to the Seventh Circuit Court of Appeals.

were covered by their health insurance and/or securing payment for the provision of such health care services." Complaint, ¶ 74.

Peters' "consumer reporting agency" allegations are more than sufficient to withstand St. Joseph's Rule 12(b)(6) motion to dismiss. Whether and to what extent St. Joseph engages in the 15 U.S.C § 1681a(f) "consumer reporting agency" activities will be confirmed via the discovery process.

Finally, Peters addressed the "furnishing" issue in her response (*id*. (Doc. #37) at 12-14), and will not repeat her arguments here. Any perceived pleading deficiencies in *Tierney* do not exist here. St. Joseph "furnished" Peters' and Class Members' PII/PHI to the data thieves. *See, e.g.*, Complaint, ¶¶ 1, 4, 23, 48, 54, 57, 59, 85, 90, 100, 105, 118, 120, 126, 137, and 141 (referring to St. Joseph's unauthorized disclosure of the PII/PHI). *See also* Peters' compendium of Complaint allegations asserting St. Joseph's disclosure of her PII/PHI at Section H of her response.

WHEREFORE, Plaintiff Beverly T. Peters, on behalf of herself and Class Members, respectfully requests this Court to (i) deny all of St. Joseph's pending motions, and (ii) grant her such other and further relief to which she is justly entitled.

Date: September 17, 2014

Respectfully submitted,

Richard L. Coffman
THE COFFMAN LAW FIRM
Texas Bar No. 04497460
Federal Bar No. 12055
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

Mitchell A. Toups
WELLER, GREEN, TOUPS & TERRELL, LLP
Texas Bar No. 20151600
Federal Bar No. 2457
2615 Calder Ave., Suite 400
Beaumont, TX 77702
Telephone: (409) 838-0101
Facsimile: (409) 838-6780
Email: matoups@wgttlaw.com

Jason Webster
THE WEBSTER LAW FIRM
Texas Bar No. 24033318
Federal Bar No. 568715
6200 Savoy, Suite 515
Houston, TX 77036
Telephone: (713) 581-3900
Facsimile: (713) 409-6464
Email: jwebster@thewebsterlawfirm.com

CERTIFICATE OF SERVICE

I certify that a true and correct copy of Plaintiff's Consolidated Surreply to Defendants' Pending Motions was served on the following counsel of record, via the Court's ECF System, on September 17, 2014.

Richard L. Coffman

Kent Adams
Kristie Johnson
LEWIS BRISBOIS BISGAARD & SMITH, LLP
24 East Greenway Plaza, Suite 1400
Houston, TX 77046
Telephone: (713) 659-6767
Facsimile: (713) 759-6830
Email: Kent.adams@lewisbrisbois.com
Email: Kristie.johnson@lewisbrisbois.com

ATTORNEYS FOR DEFENDANTS

4847-8055-9646, v. 1

Exhibit "A"

2014 WL 4379916
Only the Westlaw citation is currently available.
United States District Court,
San Jose Division.
San Jose Division

In re Adobe Systems, Inc. Privacy Litigation.

Case No.: 13-CV-05226-LHK | Signed 09/04/2014

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT ADOBE SYSTEMS INC.'S MOTION TO DISMISS

LUCY H. KOH, United States District Judge

*1 In this consolidated litigation, Plaintiffs Christian Duke ("Duke"), Joseph Kar ("Kar"), Christina Halpain ("Halpain"), Jacob McHenry ("McHenry"), Anne McGlynn ("McGlynn"), and Marcel Page ("Page"), individually and on behalf of those similarly situated (collectively, "Plaintiffs") bring claims against Defendant Adobe Systems, Inc. ("Adobe") arising out of an intrusion into Adobe's computer network in 2013 and the resulting data breach. Consol. Compl. ("Compl.") ECF No. 39. Pending before the Court is Adobe's Motion to Dismiss, in which Adobe seeks dismissal of all of Plaintiffs' claims. ("Mot.") ECF No. 45. Plaintiffs have filed an Opposition, ("Opp'n") ECF No. 47, and Adobe has filed a Reply, ("Reply") ECF No. 50. Having considered the submissions of the parties and the relevant law, the Court hereby GRANTS IN PART and DENIES IN PART Adobe's Motion to Dismiss.

I. BACKGROUND

A. Factual Allegations

Except where indicated, the facts in this section are taken from Plaintiffs' Complaint and accepted as true for the purposes of this Motion.

1. Adobe's Products and Services

Adobe is a multinational software company that sells and licenses printing, publishing, multimedia, and graphics software. Compl. ¶ 17. Adobe sells a wide range of products, including Photoshop (a widely-used digital imaging program) and ColdFusion (used by web developers to build websites and Internet applications). *Id.* ¶ 19. Adobe's products and services are available in two forms. Some Adobe software, such as ColdFusion, is sold through licenses, where customers pay a single licensing fee to use the software. *Id.* Other Adobe products are available through Adobe's subscription-based "Creative Cloud," where customers pay a monthly fee to use Adobe's products and services. *Id.*

Adobe collects a variety of customer information. Customers of licensed-based products must register their products, which requires customers to provide Adobe with their e-mail addresses and create a username and password for Adobe's website. *Id.* Some of these customers purchased their licenses online from Adobe directly, and thus also provided Adobe with their credit card numbers and expiration dates, as well as other billing information. *E.g., id.* ¶¶ 19, 78, 96. Creative Cloud customers are required to keep an active credit card on file with Adobe, which is charged automatically according to the customer's subscription plan. *Id.* ¶ 19. In addition, some Creative Cloud customers store their files and work products in Adobe's "cloud." *E.g., id.* ¶ 84. As a result of the popularity of Adobe's products, Adobe has collected personal information in the form of names, e-mail and mailing addresses, telephone numbers, passwords, credit card numbers and expiration dates from millions of customers. *Id.* ¶¶ 22, 50–55.

All customers of Adobe products, including Creative Cloud subscribers, are required to accept Adobe's End–User License Agreements ("EULA") or General Terms of Use. *Id.* ¶ 29. Both incorporate Adobe's Privacy Policy, which provides in relevant part: "[Adobe] provide[s] reasonable administrative, technical, and physical security controls to protect your information. However, despite our efforts, no security controls are 100% effective and Adobe cannot ensure or warrant the security of your personal information." ("Agreement") ECF No. 46–2 at 4. Adobe's Safe Harbor Privacy Policy, which supplements Adobe's Privacy Policy, similarly provides that "Adobe ... uses reasonable physical, electronic, and administrative safeguards to protect your personal information from loss; misuse; or unauthorized access, disclosure, alteration, or destruction." Compl. ¶ 32. Adobe makes similar representations regarding its security practices on its websites. *Id.* ¶¶ 33–39.

2. The 2013 Data Breach

***2** In July 2013, hackers gained unauthorized access to Adobe's servers. *Id.* ¶ 48. The hackers spent several weeks inside Adobe's network without being detected. *Id.* By August 2013, the hackers reached the databases containing customers' personal information, as well as the source code repositories for Adobe products. *Id.* The hackers then spent up to several weeks removing customer data and Adobe source code from Adobe's network, all while remaining undetected. *Id.* The data breach did not come to light until September, when independent security researchers discovered stolen Adobe source code on the Internet. *Id.* ¶ 49. Adobe announced the data breach on October 3, 2013. *Id.* ¶ 50. Adobe announced that the hackers accessed the personal information of at least 38 million customers, including names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and e-mail addresses. *Id.* ¶¶ 50–52. Adobe confirmed that the hackers copied the source code for a number of its products, including ColdFusion. *Id.* ¶ 53. Adobe subsequently disclosed that the hackers were able to use Adobe's systems to decrypt customers' credit card numbers, which had been stored in an encrypted form. *Id.* ¶ 57. The Court will refer to this sequence of events as the "2013 data breach."

Following the 2013 data breach, researchers concluded that Adobe's security practices were deeply flawed and did not conform to industry standards. *Id.* ¶ 59. For example, though customers' passwords had been stored in encrypted form, independent security researchers analyzing the stolen passwords discovered that Adobe's encryption scheme was poorly implemented, such that the researchers were able to decrypt a substantial portion of the stolen passwords in short order. *Id.* ¶ 63. Adobe similarly failed to employ intrusion detection systems, properly segment its network, or implement user or network level system controls. *Id.* ¶ 62. As a result of the 2013 data breach, Adobe offered its customers one year of free credit monitoring services and advised customers to monitor their accounts and credit reports for fraud and theft. *Id.* ¶¶ 54, 56.

3. The Plaintiffs

Plaintiffs are customers of Adobe licensed products or Creative Cloud subscribers who provided Adobe with their personal information. Plaintiffs Kar and Page purchased licensed products directly from Adobe and provided Adobe with their names, email addresses, credit card numbers, other billing information, and other personal information. *Id.* ¶¶ 77–78, 95–96. Plaintiff McHenry purchased an Adobe licensed product, and provided Adobe with a username and password. *Id.* ¶¶ 98–99. Plaintiffs Duke, Halpain, and McGlynn subscribed to Adobe's products, and provided Adobe with their names, email addresses, credit card numbers, other billing information, and other personal information. *Id.* ¶¶ 74–75, 83–84, 90. Plaintiffs Duke, Kar, Halpain, and McGlynn are California citizens and residents. *Id.* ¶¶ 10–12, 14. Adobe informed all Plaintiffs that their personal information had been compromised as a result of the 2013 data breach. *Id.* ¶¶ 76, 80, 85, 92, 97, 100. Following the 2013 data breach, Plaintiffs Kar and Halpain purchased additional credit monitoring services. *Id.* ¶¶ 81, 86.

B. Procedural History

The seven cases underlying this consolidated action were filed in this Court between November 2013 and January 2014. *See* ECF No. 1; Case No. 13–CV–5611, ECF No. 1; Case No. 13–CV–5596, ECF No. 1; Case No. 13–CV–5930, ECF No. 1; Case No. 14–CV–14, ECF No. 1; Case No. 14–CV–30, ECF No. 1; Case No. 14–CV–157, ECF No. 1. The Court related the individual cases in December 2013 and January 2014, ECF Nos. 19, 22, 26, [1] and consolidated them on March 13, 2014, ECF No. 34. Plaintiffs filed their Consolidated Complaint on April 4, 2014. ECF No. 39. Adobe filed its Motion to Dismiss on May 21, 2014, ECF No. 45, with an accompanying Request for Judicial Notice, ("Def. May 21 RJN") ECF No. 46. Plaintiffs filed their Opposition on June 11, 2014, ECF No. 47, with an accompanying Request for Judicial Notice, ("Pl. RJN") ECF No. 48. Adobe filed its Reply on July 2, 2014, ECF No. 50, along with a second Request for Judicial Notice, ("Def. July 2 RJN") ECF No. 51. [2]

II. LEGAL STANDARDS

A. Rule 12(b)(1)

***3** A defendant may move to dismiss an action for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1). A motion to dismiss for lack of subject matter jurisdiction will be granted if the complaint on its face fails to allege facts sufficient to establish subject matter jurisdiction. *See Savage v. Glendale Union High Sch.,* 343 F.3d 1036, 1039 n.2 (9th Cir.2003). If the plaintiff lacks standing under Article III of the U.S. Constitution, then the court lacks subject matter jurisdiction, and the case must be dismissed. *See Steel Co. v. Citizens for a Better Env't,* 523 U.S. 83, 101–02 (1998). In considering a Rule 12(b)

(1) motion, the Court "is not restricted to the face of the pleadings, but may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction." *McCarthy v. United States,* 850 F.2d 558, 560 (9th Cir.1988). Once a party has moved to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), the opposing party bears the burden of establishing the court's jurisdiction, *see Chandler v. State Farm Mut. Auto. Ins. Co.,* 598 F.3d 1115, 1122 (9th Cir.2010), by putting forth "the manner and degree of evidence required" by whatever stage of the litigation the case has reached, *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 561 (1992); *see also Barnum Timber Co. v. Envtl. Prot. Agency,* 633 F.3d 894, 899 (9th Cir.2011) (at the motion to dismiss stage, Article III standing is adequately demonstrated through allegations of "specific facts plausibly explaining" why the standing requirements are met).

B. Rule 8(a)

Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). The Supreme Court has held that Rule 8(a) requires a plaintiff to plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 570 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal,* 556 U.S. 662, 678 (2009). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, a court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.,* 519 F.3d 1025, 1031 (9th Cir.2008).

However, the Court need not accept as true allegations contradicted by judicially noticeable facts, *Shwarz v. United States,* 234 F.3d 428, 435 (9th Cir.2000), and the "[C]ourt may look beyond the plaintiff's complaint to matters of public record" without converting the Rule 12(b)(6) motion into one for summary judgment, *Shaw v. Hahn,* 56 F.3d 1128, 1129 n.1 (9th Cir.1995). Nor is the Court required to " 'assume the truth of legal conclusions merely because they are cast in the form of factual allegations.' " *Fayer v. Vaughn,* 649 F.3d 1061, 1064 (9th Cir.2011) (per curiam) (quoting *W. Mining Council v. Watt,* 643 F.2d 618, 624 (9th Cir.1981)). Mere "conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss." *Adams v. Johnson,* 355 F.3d 1179, 1183 (9th Cir.2004); *accord Iqbal,* 556 U.S. at 678. Furthermore, plaintiffs may plead themselves out of court if they "plead facts which establish that [they] cannot prevail on [their] ... claim." *Weisbuch v. Cnty. of L.A.,* 119 F.3d 778, 783 n.1 (9th Cir.1997) (internal quotation marks and citation omitted).

C. Rule 9(b)

Claims sounding in fraud or mistake are subject to the heightened pleading requirements of Federal Rule of Civil Procedure 9(b), which requires that a plaintiff alleging fraud "must state with particularity the circumstances constituting fraud." Fed.R.Civ.P. 9(b); *see Kearns v. Ford Motor Co.,* 567 F.3d 1120, 1124 (9th Cir.2009). To satisfy Rule 9(b)'s heightened standard, the allegations must be "specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." *Semegen v. Weidner,* 780 F.2d 727, 731 (9th Cir.1985). Thus, claims sounding in fraud must allege "an account of the time, place, and specific

***4** content of the false representations as well as the identities of the parties to the misrepresentations." *Swartz v. KPMG LLP,* 476 F.3d 756, 764 (9th Cir.2007) (per curiam) (internal quotation marks omitted). "The plaintiff must set forth what is false or misleading about a statement, and why it is false." *In re Glenfed, Inc. Sec. Litig.,* 42 F.3d 1541, 1548 (9th Cir.1994) (en banc), *superseded by statute on other grounds as stated in Ronconi v. Larkin,* 253 F.3d 423, 429 n.6 (9th Cir.2001).

D. Leave to Amend

If the Court determines that the complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend "should be freely granted when justice so requires," bearing in mind that "the underlying purpose of Rule 15... [is] to facilitate decision on the merits, rather than on the pleadings or technicalities." *Lopez v. Smith,* 203 F.3d 1122, 1127 (9th Cir.2000) (en banc) (internal quotation marks omitted). Nonetheless, a court "may exercise its discretion to deny leave to amend due to 'undue delay, bad faith or dilatory motive on part of the movant, repeated failure

to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party ..., [and] futility of amendment.' " *Carvalho v. Equifax Info. Servs., LLC,* 629 F.3d 876, 892–93 (9th Cir.2010) (alterations in original) (quoting *Foman v. Davis,* 371 U.S. 178, 182 (1962)).

III. DISCUSSION

Plaintiffs assert four causes of action in their Complaint. Adobe seeks dismissal of all four claims. The Court will address each claim and Adobe's corresponding objections in turn.

A. Customer Records Act Claim

Plaintiffs' first cause of action is for injunctive relief on behalf of the California Plaintiffs for violations of Sections 1798.81.5 and 1798.82 of the California Civil Code ("CRA").[3] The CRA provides in relevant part that:

> A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

Cal. Civ.Code § 1798.81.5(b). Section 1798.82, for its part, requires businesses to "disclose any breach of the security of the system following discovery or notification of the breach ... in the most expedient time possible and without unreasonable delay." Cal. Civ.Code § 1798.82(a). Plaintiffs allege that Adobe did not and does not maintain "reasonable security practices" to protect customer data, in violation of Section 1798.81.5 of the CRA, and did not promptly notify customers following the 2013 data breach, in violation of Section 1798.82 of the CRA. Compl. ¶¶ 112–113.

***5** Plaintiffs request injunctive relief pursuant to Section 1798.84(e) of the CRA, which provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined." Plaintiffs also base their request for relief on the "unlawful" prong of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof.Code §§ 17200 *et seq.,* which allows plaintiffs to "borrow" violations of other laws and treat them as unlawful competition that is independently actionable. *Cel-Tech Commcn's, Inc. v. L.A. Cellular Tel. Co.,* 20 Cal.4th 163, 180 (1999).

Adobe argues that Plaintiffs do not allege injury-in-fact resulting from Adobe's alleged violation of the CRA and thus do not have Article III standing to bring their CRA claim. Mot. at 6–7. For the same reasons, Adobe contends that Plaintiffs do not have statutory standing under Section 1798.84(e), which also requires a showing of injury. *Id.* As a result, Adobe contends that Plaintiffs' CRA claim must be dismissed for lack of jurisdiction. The Court addresses both contentions in turn, beginning, as it must, with Article III standing.

1. Article III Standing

To have Article III standing, a plaintiff must plead and prove that she has suffered sufficient injury to satisfy the "case or controversy" requirement of Article III of the United States Constitution. *See Clapper v. Amnesty Int'l USA,* ––– U.S. ––––, 133 S.Ct. 1138, 1146 (2013) (" 'One element of the case-or-controversy requirement' is that plaintiffs 'must establish that they have standing to sue.' " (quoting *Raines v. Byrd,* 521 U.S. 811, 818 (1997))). To satisfy Article III standing, a plaintiff must therefore allege: (1) injury-in-fact that is concrete and particularized, as well as actual or imminent; (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that the injury is redressable by a favorable ruling. *Monsanto Co. v. Geertson Seed Farms,* 561 U.S. 139, 149 (2010); *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.,* 528 U.S. 167, 180–81 (2000). "The party invoking federal jurisdiction bears the burden of establishing these elements ... with the manner and degree of evidence required at the successive stages of the litigation." *Lujan,* 504 U.S. at 561.

In a class action, named plaintiffs representing a class "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent." *Warth v. Seldin,* 422 U.S. 490, 502 (1975). "[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class." *O'Shea v. Littleton,* 414 U.S. 488, 494 (1974).

In the instant case, Plaintiffs allege that they have all suffered at least one of three types of cognizable injuries-in-fact: (1) increased risk of future harm; (2) cost to mitigate the risk of future harm; and/or (3) loss of the value of their Adobe products. Opp'n at 7–11. The Court begins by assessing the adequacy Plaintiffs' alleged injuries. The Court will then address Adobe's argument that even if Plaintiffs have Article III standing to bring a claim based on Adobe's alleged violation of Section 1798.81.5 (the "reasonable" security measures provision), Plaintiffs do not have standing to bring a claim based on Adobe's alleged violation of Section 1798.82 (the notification provision), because Plaintiffs do not allege that they suffered any particular injury stemming from Adobe's failure to reasonably *notify* Plaintiffs of the 2013 data breach. Mot. at 7.

a. Increased Risk of Harm

***6** Plaintiffs claim that they are all at increased risk of future harm as a result of the 2013 data breach. Opp'n at 7. Adobe counters that such "increased risk" is not a cognizable injury for Article III standing purposes. Mot. at 10. The Ninth Circuit addressed Article III standing in the context of stolen personal information in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir.2010). In *Krottner*, a thief stole a laptop from Starbucks containing the unencrypted names, addresses, and social security numbers of roughly 97,000 Starbucks employees. *Id.* at 1140. Some of the affected employees subsequently sued Starbucks for negligence and breach of implied contract. *Id.* Starbucks argued that the employees did not have standing because there was no indication that any of the employees' personal information had been misused or that the employees had suffered any economic loss as a result of the theft. *Id.* at 1141–42. The Ninth Circuit disagreed, holding instead that "the possibility of future injury may be sufficient to confer standing" where the plaintiff is "*immediately* in danger of sustaining some *direct* injury as the result of the challenged conduct." *Id.* at 1142 (alteration omitted) (internal quotation marks omitted). As to the specific facts before it, the Ninth Circuit held that the Starbucks employees alleged "a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." *Id.* at 1143. Based on this "credible threat of real and immediate harm," the Ninth Circuit found that the employees "sufficiently alleged an injury-in-fact for purposes of Article III standing." *Id.*

Adobe does not dispute that *Krottner* is directly on point. *See* Mot. at 11; Reply at 3. However, Adobe contends that subsequent Supreme Court authority forecloses the approach the Ninth Circuit took to standing in *Krottner*. Reply at 3. Specifically, Adobe claims that the Supreme Court's decision in *Clapper v. Amnesty International USA* expressly rejected "[a]llegations of *possible* future injury" as a basis for Article III standing, requiring instead that a "threatened injury [ ] be *certainly impending* to constitute injury in fact." Mot. at 10 (citing *Clapper,* 133 S.Ct. at 1147). Adobe argues that following *Clapper* district courts in data breach cases regularly conclude that increased risk of future harm is insufficient to confer Article III standing under the "certainly impending" standard. *Id.* (citing *In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.* ("*SAIC* "), ––– F.Supp.2d ––––, 2014 WL 1858458 (D.D.C. May 9, 2014); *Strautins v. Trustwave Holdings, Inc.*, ––– F.Supp.2d ––––, 2014 WL 960816 (N.D.Ill. Mar. 12, 2014); *Galaria v. Nationwide Mut. Ins. Co.*, ––– F.Supp.2d ––––, 2014 WL 689703 (S.D.Ohio Feb. 10, 2014); *Polanco v. Omnicell, Inc.*, 988 F.Supp.2d 451 (D.N.J.2013); *In re Barnes & Noble Pin Pad Litig.*, No. 12–8617, 2013 WL 4759588 (N.D.Ill. Sep. 3, 2013); *Yunker v. Pandora Media, Inc.*, No. 11–3113, 2013 WL 1282980 (N.D.Cal. Mar. 26, 2013)). Adobe claims that the only case to hold otherwise, *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, ––– F.Supp.2d ––––, 2014 WL 223677 (S.D. Cal. Jan 21, 2014), has been "relegated to a '*but see* ' reference." Mot. at 11 (citing *SAIC*, 2014 WL 1858458, at *8). Adobe encourages this Court to conclude that *Clapper* implicitly overruled *Krottner* and to join the district courts that have rejected the "increased risk of harm" theory of standing in *Clapper* 's wake. *Id.* at 10–11. For the following reasons, the Court declines to do so.

Clapper addressed a challenge to Section 702 of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. § 1881a. 133 S.Ct. at 1142. Respondents were U.S.-based attorneys, human rights, labor, legal, and media organizations who alleged that their work required them to communicate with individuals outside the United States who were likely to be targets of surveillance under Section 702. Id. at 1145. The respondents asserted injury based on "an objectively reasonable likelihood that their communications [would] be acquired [under FISA] at some point in the future." Id. at 1146. As an initial matter, the Supreme Court held that the "objectively reasonable likelihood" standard was inconsistent with precedent requiring that "threatened injury must be certainly impending to constitute injury in

fact." Id. at 1147 (emphasis added) (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)). The Supreme Court emphasized that "allegations of possible future injury are not sufficient." Id. (internal quotation marks omitted). Turning to the respondents' theory of injury, the Supreme Court found that it was both too speculative to constitute "certainly impending" injury and too attenuated to be "fairly traceable" to Section 702. Id. at 1147–48.

*7 As the Supreme Court noted, the respondents did not allege that any of their communications had actually been intercepted, or even that the Government sought to target them directly. *Id.* at 1148. Rather, the respondents' argument rested on the "highly speculative fear" that:

> (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under [Section 702] rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy [Section 702]'s many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts

Id.The Supreme Court held that this "highly attenuated" chain of possibilities did not result in a "certainly impending" injury. Id. The Court observed that the first three steps of the chain depended on the independent choices of the Government and the Foreign Intelligence Surveillance Court, yet the respondents could only speculate as to what decision those third parties would take at each step. *Id.* at 1149–50 ("[W]e have been reluctant to endorse standing theories that require guesswork as to how independent decisionmakers will exercise their judgment...."). Moreover, respondents could not show with any certainty that *their* communications with the foreign persons allegedly under surveillance would be intercepted. *Id.* As a result, the overall chain of inferences was "too speculative" to constitute a cognizable injury. *Id.* at 1143.

The Supreme Court acknowledged that its precedents "do not uniformly require plaintiffs to demonstrate that it is *literally certain* that the harms they identify will come about" in order to have standing. *Id.* at 1150 n.5 (emphasis added). Rather, in some cases, the Supreme Court has found standing "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Id.* (citing *Monsanto,* 561 U.S. at 153–54; *Pennell v. City of San Jose,* 485 U.S. 1, 8 (1988); *Blum v. Yaretsky,* 457 U.S. 991, 1000–01 (1982); *Babbitt v. Farm Workers,* 442 U.S. 289, 298 (1979)). The Supreme Court declined to overrule that line of cases. However, the Court concluded in *Clapper* that "to the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement, respondents fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm here." *Id.*

Clapper did not change the law governing Article III standing. The Supreme Court did not overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact, causation, and redressability. [4] Accord Sony, 2014 WL 223677, at *8–9 ("[T]he Supreme Court's decision in Clapper did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent...."). Clapper merely held that the Second Circuit had strayed from these well-established standing principles by accepting a too-speculative theory of future injury. See 133 S.Ct. at 1146 (characterizing the Second Circuit's view of standing as "novel"). In the absence of any indication in Clapper that the Supreme Court intended a wide- reaching revision to existing standing doctrine, the Court is reluctant to conclude that *Clapper* represents the sea change that Adobe suggests. Moreover, *Clapper* 's discussion of standing arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result. *Id.* at 1147 ("Our standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."(alteration omitted) (internal quotation marks omitted)).

*8 "[D]istrict courts should consider themselves bound by [ ] intervening higher authority and reject the prior

opinion of [the Ninth Circuit] as having been effectively overruled" only when the intervening higher authority is "clearly irreconcilable with [the] prior circuit authority." *Miller v. Gammie,* 335 F.3d 889, 900 (9th Cir.2003) (en banc). The Court does not find that *Krottner* and *Clapper* are clearly irreconcilable. *Krottner* did use somewhat different phrases to describe the degree of imminence a plaintiff must allege in order to have standing based on a threat of injury, *i.e.,*"immediate[ ][ ] danger of sustaining some direct injury," and a "credible threat of real and immediate harm." 628 F.3d at 1142–43. On the other hand, *Clapper* described the harm as "certainly impending." 133 S.Ct. at 1147. However, this difference in wording is not substantial. At the least, the Court finds that *Krottner* 's phrasing is closer to *Clapper* 's "certainly impending" language than it is to the Second Circuit's "objective reasonable likelihood" standard that the Supreme Court reversed in *Clapper*. Given that *Krottner* described the imminence standard in terms similar to those used in *Clapper,* and in light of the fact that nothing in *Clapper* reveals an intent to alter established standing principles, the Court cannot conclude that *Krottner* has been effectively overruled.

In any event, even if *Krottner* is no longer good law, the threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*. Unlike in *Clapper,* where respondents' claim that they would suffer future harm rested on a chain of events that was both "highly attenuated" and "highly speculative," 133 S.Ct. at 1148, the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real. Plaintiffs allege that the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates. Compl. ¶¶ 48, 50. Plaintiffs' personal information was among the information taken during the breach. *Id.* ¶¶ 76, 80, 85, 92, 97, 100. Thus, in contrast to *Clapper,* where there was no evidence that any of respondents' communications either had been or would be monitored under Section 702, *see* 133 S.Ct. at 1148, here there is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken.

Neither is there any need to speculate as to whether the hackers intend to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so. Not only did the hackers deliberately target Adobe's servers, but Plaintiffs allege that the hackers used Adobe's own systems to decrypt customer credit card numbers. Compl. ¶ 57. Some of the stolen data has already surfaced on the Internet, and other hackers have allegedly misused it to discover vulnerabilities in Adobe's products. *Id.* ¶¶ 49, 70. Given this, the danger that Plaintiffs' stolen data will be subject to misuse can plausibly be described as "certainly impending." Indeed, the threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused. However, to require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be "literally certain" in order to constitute injury-in-fact.[5] *Clapper,* 133 S.Ct. at 1150 n.5; *see also, e.g.,Monsanto,* 561 U.S. at 153–54 (finding that a "substantial risk of gene flow" from genetically engineered alfalfa crops to non-genetically engineered alfalfa crops was sufficient to confer Article III standing).[6]

***9** The cases Adobe cites in which district courts have relied on *Clapper* to dismiss data breach cases on standing grounds are factually distinct from the present case. In *SAIC,* the case on which Adobe most heavily relies, a thief broke into a car in San Antonio, Texas and stole the car's GPS and stereo, as well as encrypted backup data tapes containing personal medical information for over four million U.S. military members and their families. 2014 WL 1858458, at *2. As the *SAIC* court found, the thief would need to have recognized the data tapes for what they were, obtained specialized equipment to read the tapes, broken the encryption protecting the data on the tapes, and then obtained specialized software to read the data, all before being in any position to misuse the data. *Id.* at *6. Such a chain of possibilities, the *SAIC* court held, was as attenuated as the chain the Supreme Court rejected in *Clapper,* especially given the more likely possibility that the thief had simply sold the GPS and stereo and discarded the data tapes "in a landfill somewhere in Texas." *Id.* The facts of *SAIC* stand in sharp contrast to those alleged here, where hackers targeted Adobe's servers in order to steal customer data, at least some of that data has been successfully decrypted, and some of the information stolen in the 2013 data breach has already surfaced on websites used by hackers.

Adobe's other authorities are similarly distinct. The thief in *Polanco* also stole a laptop out of a car. 988 F.Supp.2d at 456. Again, there was no allegation that the thief targeted the laptop for the data contained therein, and the plaintiff "essentially concede[d]" that she had not alleged "any misuse of her [personal information] or [ ] that she [wa]s now at an increased risk for the misuse of her information in the

future based on the theft of the laptop." *Id.* at 467. In both *Strautins* and *Barnes & Noble,* it was unclear if the plaintiffs' information had been taken at all. 2014 WL 960816, at *6–7; 2013 WL 4759588, at *4. Finally, in *Yunker,* the plaintiff did not allege that he had provided any sensitive information (such as a credit card number or a social security number) or that anyone had breached the defendant's servers. 2013 WL 1282980, at *5.

The case with facts closest to those at issue here is *Galaria.* In that case, hackers obtained a variety of personal information, though not credit card information, from the servers of an insurance company. *Galaria,* 2014 WL 689703, at * 1. The court declined to find standing based on increased risk of future harm, reasoning that whether plaintiffs would be harmed depended on the decision of the unknown hackers, who may or may not attempt to misuse the stolen information. Id. at *6. The Court finds this reasoning unpersuasive–after all, why would hackers target and steal personal customer data if not to misuse it?–and declines to follow it. Regardless, Galaria's reasoning lacks force here, where Plaintiffs allege that some of the stolen data has already been misused. See Compl. ¶¶ 49, 70.

In sum, the Court finds that Plaintiffs' allegations of a concrete and imminent threat of future harm suffice to establish Article III injury-in-fact at the pleadings stage under both *Krottner* and *Clapper.*

b. Cost to Mitigate

In addition, Plaintiffs allege that Plaintiffs Halpain and Kar have standing based on the reasonable costs they incurred to mitigate the increased risk of harm resulting from the 2013 data breach. Opp'n at 10; *see* Compl. ¶¶ 80–81, 86–87 (alleging that Halpain and Kar paid for data monitoring services). The Supreme Court held in Clapper that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 133 S.Ct. at 1151. In so holding, the Supreme Court rejected the *Clapper* respondents' argument that they had standing because they had taken on costly and burdensome measures to protect the confidentiality of their communications. *Id.* Even where the fear of harm was not "fanciful, paranoid, or otherwise unreasonable," the Supreme Court noted, plaintiffs cannot secure a lower standard for standing "simply by making an expenditure based on [that] fear." *Id.*

As this last quote indicates, the Supreme Court's primary concern was that the Article III standing standard would be "water[ed] down" if a plaintiff who otherwise lacked standing could manufacture an injury-in-fact "for the price of a plane ticket." *Id.* (internal quotation marks omitted); *accord SAIC,* 2014 WL 1858458, at *7 ("Put another way, the [Supreme] Court has held that plaintiffs cannot create standing by 'inflicting harm on themselves' to ward off an otherwise speculative injury."(quoting *Clapper,* 133 S.Ct. at 1151)). Therefore, in order for costs incurred in an effort to mitigate the risk of future harm to constitute injury-in-fact, the future harm being mitigated must itself be imminent. [7] As the Court has found that all Plaintiffs adequately alleged that they face a certainly impending future harm from the theft of their personal data, *see supra* Part III.A.1.a, the Court finds that the costs Plaintiffs Halpain and Kar incurred to mitigate this future harm constitute an additional injury-in-fact. [8]

***10** For the foregoing reasons, the Court finds that Plaintiffs have plausibly alleged that the substantial risk of harm Plaintiffs face following the 2013 data breach constitutes a cognizable injury-in-fact. The costs Plaintiffs Halpain and Kar incurred to mitigate this risk of harm constitute an additional cognizable injury. The Court further finds that Plaintiffs plausibly allege both that these injuries are "fairly traceable" to Adobe's alleged failure to maintain "reasonable" security measures in violation of Section 1798.81.5 and that the relief sought would redress these injuries. The Court therefore concludes that Plaintiffs have adequately pleaded that they have Article III standing to bring a CRA claim for violations of Section 1798.81.5.

c. Section 1798.82

Adobe argues that even if Plaintiffs have adequately alleged injury-in-fact stemming from Adobe's alleged failure to implement reasonable security measures, Plaintiffs have not alleged any injury traceable to Adobe's alleged failure to reasonably *notify* customers of the 2013 data breach in violation of Section 1798.82, because Plaintiffs do not allege that they suffered any incremental harm as a result of the delay. Mot. at 7. The Court agrees that Plaintiffs do not allege any harm resulting from the delay in their Complaint, and Plaintiffs do not address this argument in their Opposition except to argue that they have statutory (as opposed to Article III) standing to bring a Section 1798.82 claim. *See* Opp'n at 11.

Article III's standing requirements are mandatory and separate from any statutory standing requirements. Article III standing is also claim- and relief-specific, such that a plaintiff must establish Article III standing for each of her claims and for each form of relief sought. *See DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) ("[O]ur standing cases confirm that a plaintiff must demonstrate standing for each claim he seeks to press."); *id.* ("We have insisted ... that a plaintiff must demonstrate standing separately for each form of relief sought."(internal quotation marks omitted)). Plaintiffs' claim that Adobe failed to reasonably notify its customers of the 2013 data breach is distinct from Plaintiffs' claim that Adobe failed to maintain reasonable data security measures–in that the claims arise under different statutory provisions and challenge different Adobe conduct–and Plaintiffs seek different injunctive relief to remedy each violation. *Compare* Compl. ¶ 116 (seeking injunction ordering Adobe to implement various security measures), *with id.* ¶ 117 (seeking injunction ordering Adobe to notify customers affected by the 2013 data breach who have not yet received notice that their data was stolen). Thus, the Court concludes that Plaintiffs must separately establish Article III standing under Section 1798.82. However, by failing to allege any injury resulting from a failure to provide reasonable notification of the 2013 data breach, Plaintiffs have not plausibly alleged that they have standing to pursue a Section 1798.82 claim. Accordingly, the Court GRANTS Adobe's Motion to Dismiss Plaintiffs' Section 1798.82 claim for lacking of Article III standing. Because Plaintiffs may be able to cure this deficiency in an amended complaint, this dismissal is without prejudice.

2. Statutory Standing

The CRA also contains a statutory standing requirement. Section 1798.84, the remedies provision of the CRA, provides that "[a]ny customer injured by a violation of this title may institute a civil action to recover damages,"Cal. Civ.Code § 1798.84(b), and the California Court of Appeal has held that this injury requirement applies "regardless of the remedies [a plaintiff] seek [s],"*Boorstein v. CBS Interactive, Inc.*, 222 Cal.App. 4th 456, 466–67 (2013); *accord Murray v. Time Inc.*, 554 F. App'x 654, 655 (9th Cir.2014). Therefore, where a plaintiff fails to allege a cognizable injury, the plaintiff "lacks statutory standing" to bring a claim under Section 1798.84, "regardless of whether [the] allegations are sufficient to state a violation of the [statute]." *Boorstein*, 222 Cal.App. 4th at 467 (internal quotation marks omitted).

***11** Although Section 1798.84 does not define what qualifies as an injury under the statute, other courts in the Ninth Circuit have found that an injury that satisfies Article III's injury-in-fact standard suffices to establish statutory injury under the CRA. *See, e.g.,Miller v. Hearst Commc'ns, Inc.*, No. 12–733, 2012 WL 3205241, at *6 (C.D.Cal. Aug. 3, 2012); *Boorstein v. Men's Journal LLC*, No 12–771, 2012 WL 2152815, at *3–4 (C.D. Cal. June 14, 2012). As Adobe does not contend, and as the Court has no reason to believe, that the CRA's statutory standing requirements are more stringent than Article III's, the Court finds that Plaintiffs' allegations of injury-in-fact satisfy the CRA's statutory standing requirement for the same reasons these allegations satisfy Article III. *See supra* Part III.A.1.

In summary, the Court DENIES Adobe's Motion to Dismiss Plaintiffs' CRA claim for violations of Section 1798.81.5. The Court GRANTS Adobe's Motion to Dismiss Plaintiffs' CRA claim for violations of Section 1798.82 without prejudice.

B. Declaratory Relief

Plaintiffs' second cause of action is for declaratory relief on behalf of all Plaintiffs. Compl. ¶¶ 118–124. As a preliminary matter, the parties disagree over whether the federal Declaratory Judgment Act, 28 U.S.C. § 2201, applies, as Adobe contends, or if the California Declaratory Relief Act, Cal.Civ.Proc.Code § 1060, applies, as Plaintiffs contend. *Compare* Reply at 5 n.4, *with* Opp'n at 14.

The Court finds that the federal Declaratory Judgment Act governs in this case. Although district courts in the Ninth Circuit have at times applied the California Declaratory Relief Act when sitting in diversity, *see Valley Forge Ins. Co. v. APL Co. Pte. Ltd.*, No. 09–9323, 2010 WL 960341, at *4 n.5 (C.D.Cal. Mar. 16, 2010) (citing cases), other district courts apply the federal Act, *see, e.g.,DeFeo v. Procter & Gamble Co.*, 831 F.Supp. 776, 779 (N.D.Cal.1993) ("The propriety of granting declaratory relief in federal court is a procedural matter.... Therefore, the Declaratory Judgment Act is implicated even in diversity cases ...." (citations omitted)). For its part, the Ninth Circuit has indicated, although not explicitly held, that the federal Declaratory Judgment Act should apply. In *Golden Eagle Insurance Co. v. Travelers Cos.*, 103 F.3d 750, 753 (9th Cir.1996), *overruled on other grounds byGov't Emps. Ins. Co. v. Dizol*, 133 F.3d 1220 (1998) (en banc), the Ninth Circuit stated

that although "[t]he complaint [plaintiff] filed in state court was for declaratory relief under California's declaratory relief statute," "[w]hen [defendant] removed the case to federal court, based on diversity of citizenship, the claim remained one for declaratory relief, but the question whether to exercise federal jurisdiction to resolve the controversy became a procedural question of federal law." Finally, the U.S. Supreme Court has emphasized the procedural nature of the Declaratory Judgment Act, which further supports the conclusion that the federal Act applies. *See Skelly Oil Co. v. Phillips Petroleum Co.,* 339 U.S. 667, 671 (1950) (" '[T]he operation of the Declaratory Judgment Act is procedural only.' " (quoting *Aetna Life Ins. Co. v. Haworth,* 200 U.S. 227, 240 (1937))). The Court will therefore consider Plaintiffs' declaratory relief claim under the federal Declaratory Judgment Act. In any event, as Plaintiffs acknowledge, whether the state or federal statute applies makes little difference as a practical matter, as the two statutes are broadly equivalent. [9] *See* Opp'n at 14.

***12** The federal Declaratory Judgment Act provides that "[i]n a case of actual controversy within its jurisdiction ... any court of the United States ... may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought." 28 U.S.C. § 2201(a). To fall within the Act's ambit, the "case of actual controversy" must be " 'definite and concrete, touching the legal relations of parties having adverse legal interests,'... 'real and substantial' and 'admi[t] of specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts.' " *MedImmune, Inc. v. Genentech, Inc.,* 549 U.S. 118, 127 (2007) (alteration in original) (quoting *Aetna Life,* 300 U.S. at 240–241). Plaintiffs seek a declaration that: (a) Adobe fails to fulfill its existing contractual obligation to provide reasonable security measures; and (b) to comply with its contractual obligations, Adobe must implement specified additional security measures. Compl. ¶ 124.

Adobe moves to dismiss Plaintiff's declaratory relief claim on three grounds. First, Adobe asserts that Plaintiffs have not suffered an injury-in-fact and therefore lack standing. Mot. at 13. Second, Adobe contends that what Plaintiffs actually seek is an impermissible advisory opinion that lays the foundation for future litigation, rather than adjudication of an actual controversy between the parties. *Id.* at 13–14. Third, Adobe argues that Plaintiffs' declaratory relief claim is actually a breach of contract claim in disguise, and that the claim fails because Plaintiffs have failed to plead all the elements of a breach of contract claim. *Id.* at 15. The Court addresses each contention in turn.

1. Article III Standing

Adobe first claims that, just as the California Plaintiffs fail to allege injury-in-fact for purposes of their CRA claim, the California Plaintiffs fail to allege a cognizable injury-in-fact for purposes of declaratory relief. Mot. at 13; *see also Dizol,* 133 F.3d at 1222–23 ("A lawsuit seeking federal declaratory relief must first present an actual case or controversy within the meaning of Article III, section 2 of the United States Constitution.... It must also fulfill statutory jurisdictional prerequisites."(citation omitted)). In addition, Adobe claims that the non-California Plaintiffs do not allege any injury whatsoever. Mot. at 13. Adobe argues that therefore none of the Plaintiffs alleges injury-in-fact that is fairly traceable to Adobe's failure to abide by its contractual obligations. *Id.*

The Court finds that Plaintiffs have adequately pleaded that they have Article III standing to bring a claim for declaratory relief. First, as discussed above, the Court finds that all Plaintiffs have plausibly alleged that they face a substantial, "certainly impending" risk of harm from the 2013 data breach. *See supra* Part III.A. 1.a. This alleged injury is fairly traceable to Adobe's failure to abide by its contractual obligation to provide "reasonable ... security controls," Agreement at 4, and will plausibly be redressed by the declaratory relief Plaintiffs seek. Accordingly, the Court declines to dismiss Plaintiffs' declaratory relief claim for lack of Article III standing.

2. Presence of an Actionable Dispute

Adobe next seeks dismissal of Plaintiffs' declaratory relief claim on the ground that Plaintiffs do not fulfill the Declaratory Judgment Act's statutory jurisdictional requirements. Adobe contends that there is no actionable dispute over whether Adobe is in breach of its contractual obligation to provide "reasonable .... security controls," given that the Agreement expressly provides that no security measure is "100%" effective and that "Adobe cannot ensure or warrant the security of your personal information." Mot. at 14. Adobe further contends that Plaintiffs do not allege that a declaration of rights is necessary at this time. *Id.* Adobe asserts that Plaintiffs' claim is consequently unripe, and is

instead a request for an impermissible advisory opinion. *Id.* Adobe contends that what Plaintiffs actually seek is an advantage for future litigation by obtaining an "advance ruling." *Id.*

***13** A claim for relief under the Declaratory Judgment Act requires a dispute that is: (1) "definite and concrete, touching the legal relations of parties having adverse legal interests"; (2) "real and substantial"; and (3) "admit[ting] of specific relief through a decree of a conclusive character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts." *MedImmune,* 549 U.S. at 127 (internal quotation marks omitted). The Supreme Court has admitted that "not ... the brightest of lines" separates cases that satisfy the statutory jurisdictional requirements and those that do not. *Id.* The central question, however, is whether " 'the facts alleged, under all the circumstances, show that there is a substantial controversy, between parties having adverse legal interests, of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.' " *Id.* (quoting *Md. Cas. Co. v. Pac. Coal & Oil Co.,* 312 U.S. 270, 273 (1941)).

The Court finds that Plaintiffs have adequately alleged the existence of an actionable dispute for purposes of the Declaratory Judgment Act. Plaintiffs have plausibly alleged the existence of a "definite and concrete" dispute over the meaning and the scope of Adobe's contractual obligation to provide "reasonable" security measures. *See* Compl. ¶¶ 120–123. According to the Complaint, although "Adobe maintains that its security measures were adequate and remain adequate," there were in fact a number of standard industry practices that Adobe failed to follow. *Id.* ¶¶ 62, 123–124. Although Adobe contends that there can be no actionable dispute concerning the adequacy of Adobe's security controls because the Agreement expressly provides that no security measure is "100%" effective, Mot. at 14, this disclaimer does not relieve Adobe of the responsibility (also contained in the Agreement) to provide "reasonable" security, *see* Agreement at 4; Compl. ¶ 120.

The remaining jurisdictional prerequisites for a declaratory relief claim are met here as well. The dispute over the reasonableness of Adobe's security controls touches on the parties' legal relations, and the parties' legal interests are adverse. *See MedImmune,* 549 U.S. at 127. Plaintiffs plausibly allege that they face a substantial risk of future harm if Adobe's security shortcomings are not redressed, making this dispute sufficiently real and immediate, [10] and the dispute underlying Plaintiffs' declaratory relief claim concerns Adobe's current security practices, rather than a hypothetical set of acts or omissions. [11] *See id.*

***14** Adobe contends that Plaintiffs seek an impermissible advisory opinion, claiming that Plaintiffs admit that declaratory relief is necessary "only so that users ... who suffer identity theft ... will not have to individually re-litigate the technical issue of Adobe's security obligations." Mot. at 14 (emphasis removed) (citing Compl. ¶ 5). Adobe is correct that declaratory relief claims brought solely for the purpose of gaining an advantage for future litigation are impermissible. *See Calderon v. Ashmus,* 523 U.S. 740, 747 (1998). However, Plaintiffs are not seeking an advance ruling on whether Adobe's security practices in 2013 were reasonable at that time. Rather, the dispute is over Adobe's *current* practices. Compl. ¶ 124 ("Plaintiffs ... seek a declaration [ ] that Adobe's *existing* security measures do not comply with its contractual obligations ...." (emphasis added)). Thus, the Court finds that Plaintiffs' declaratory relief claim does not merely seek an advisory opinion for use in future breach of contract actions.

The Court concludes that Plaintiffs have plausibly alleged that they satisfy the statutory jurisdictional requirements for obtaining declaratory relief. Adobe is not entitled to dismissal of Plaintiffs' claim on this basis.

3. Breach of Contract Claim in "Disguise"

Adobe's third and final challenge to Plaintiffs' declaratory relief claim is that Plaintiffs are "seeking a declaration that Adobe has breached its contractual obligations" without having alleged all the elements of a breach of contract claim. Mot. at 15. Relying on *Gamble v. GMAC Mortgage Corp.,* No. 08–5532, 2009 WL 400359 (N.D.Cal. Feb. 18, 2009), and*Household Financial* Services, Inc. v. Northern Trade Mortgage Corp., No. 99–2840, 1999 WL 782072 (N.D.Ill. Sept. 27, 1999), Adobe contends that Plaintiffs' claim therefore falls outside the scope of the Declaratory Judgment Act. Id.

Adobe mischaracterizes Plaintiffs' declaratory relief claim. In both *Gamble* and *Household Financial,* the plaintiffs sought a judicial decree stating that the defendants had breached their contractual obligations. *Gamble,* 2009 WL 400359, at *2 ("[P]laintiffs want the court to issue a declaratory judgment declaring that defendants breached the forbearance agreements"); *Household Fin.,*1999 WL 782072, at *3 ("Plaintiff does not request the court to clarify the parties'

rights under the loan purchase agreement. Rather, plaintiff requests a judicial declaration that defendant breached the agreement."). That is not what Plaintiffs seek here. As discussed above, Plaintiffs seek a declaration clarifying Adobe's *ongoing* contractual obligation to provide reasonable security. Opp'n at 15; Compl. ¶ 124 ("Plaintiffs ... seek a declaration [ ] that Adobe's *existing* security measures do not comply with its contractual obligations ...." (emphasis added)). Plaintiffs' claim thus requests precisely the type of relief that the Declaratory Judgment Act is supposed to provide: a declaration that will prevent future harm from ongoing and future violations before the harm occurs. *See, e.g. Minn. Min. & Mfg. Co. v. Norton Co.*, 929 F.2d 670, 673 (Fed.Cir.1991) ("In promulgating the Declaratory Judgment Act, Congress intended to prevent avoidable damages from being incurred by a person uncertain of his rights and threatened with damage by delayed adjudication."). As the Court finds that Plaintiffs are not seeking a declaration that Adobe was in breach of a contract at the time of the 2013 data breach, the Court concludes that Plaintiffs are not required to plead the elements of a breach of contract claim. The Court therefore declines to dismiss Plaintiffs' declaratory relief claim on this basis.

For the foregoing reasons, the Court finds that Plaintiffs have plausibly pleaded that they fulfill both Article III's standing requirements and the statutory jurisdictional requirements of the Declaratory Judgment Act. The Court also finds that Plaintiffs have plausibly stated a claim for declaratory relief. Accordingly, the Court DENIES Adobe's Motion to Dismiss Plaintiffs' declaratory relief claim.

C. UCL Injunction Claim

***15** Plaintiffs' third cause of action is for injunctive relief under the UCL on behalf of all Plaintiffs ("UCL injunction claim"). *See* Compl. ¶¶ 125–132. The UCL creates a cause of action for business practices that are: (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof.Code §§ 17200 *et seq.* The UCL's coverage is "sweeping," and its standard for wrongful business conduct is "intentionally broad." *In re First Alliance Mortg. Co.*, 471 F.3d 977, 995 (9th Cir.2006) (internal quotation marks omitted). Each prong of the UCL provides a separate and distinct theory of liability. *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir.2007). To assert a UCL claim, a private plaintiff must have "suffered injury in fact and ... lost money or property as a result of the unfair competition." *Rubio v. Capital One Bank*, 613 F.3d 1195, 1203 (9th Cir.2010) (quoting Cal. Bus. & Prof.Code § 17204). Plaintiffs assert claims under both the "unfair" and "unlawful" prongs of the UCL. Compl. ¶ 126.

Adobe seeks dismissal of Plaintiffs' UCL injunction claim on three grounds. First, Adobe contends that Plaintiffs lack standing to bring this claim. Mot at 16. Second, Adobe contends that Plaintiffs impermissibly seek a contract remedy without bringing a breach of contract claim. *Id.* Finally, Adobe contends that Plaintiffs have failed to allege any conduct that is unfair or unlawful within the meaning of the UCL. *Id.* The Court addresses each of Adobe's contentions below.

1. Standing

Adobe argues that, just as with Plaintiffs' CRA and declaratory relief claims, Plaintiffs lack Article III standing to bring their UCL injunction claim because no Plaintiff has suffered an injuryin-fact. *Id.* For the same reason, Adobe contends that Plaintiffs lack statutory standing to bring a claim under the UCL. *Id.* The Court finds that Plaintiffs have Article III standing to bring their UCL injunction claim for the same reasons that Plaintiffs have Article III standing to bring their CRA and declaratory relief claims. *See supra* Part III.A.1; Part III.B.1.

Adobe further argues that Plaintiffs lack statutory standing under the UCL. Mot. at 16. In order to establish standing for a UCL claim, plaintiffs must show they personally lost money or property "as a result of the unfair competition." Cal. Bus. & Prof.Code § 17204; *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 330 (2011). "There are innumerable ways in which economic injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *Id.* at 323.

Four of the six Plaintiffs allege they personally spent more on Adobe products than they would had they known Adobe was not providing the reasonable security Adobe represented it was providing. *See* Compl. ¶ 79 ("Had Mr. Kar known that Adobe's security practices were inferior to industry standard security practices, he would not have purchased [a] license online ...."); *id.* ¶ 84 ("Had Ms.

Halpain known that Adobe employed substandard security practices, she would not have subscribed to the Creative Cloud service."); *id.* ¶ 91 ("Had Ms. McGlynn known that Adobe employed substandard security practices, she would not have subscribed to the Creative Cloud Service."); *id.* ¶¶ 98–99 ("McHenry purchased Adobe Illustrator ... for approximately $579.99 .... [He] relied on Adobe's Privacy Policy and believed that Adobe would provide reasonable security...."). Only Plaintiffs Duke and Page do not allege this or any other UCL injury.

***16** The Court finds plausible Plaintiffs Kar, Halpain, McGlynn, and McHenry's allegations that they relied on Adobe's representations regarding security to their detriment. The parties agree that every Plaintiff was required to accept Adobe's Privacy Policy before creating an account or providing Adobe with their personal information. Compl. ¶¶ 31–32; Mot. at 3. In that policy, Adobe represented that it would provide reasonable measures to protect customers' personal identifying and financial information. *See* Mot. at 12. It is also plausible that a company's reasonable security practices reduce the risk of theft of customer's personal data and thus that a company's security practices have economic value. *See Kwikset,* 51 Cal.4th at 330 (Plaintiffs can establish UCL standing by alleging they paid more than they actually valued the product); *see also In re iPhone Application Litig.,* 844 F.Supp.2d 1040, 1072 (N.D.Cal.2012) (finding UCL standing was adequately pleaded where plaintiffs claimed they paid more for iPhones than they would if they had known of defendant's alleged misrepresentations or omissions).

Accordingly, the Court finds that Plaintiffs Kar, Halpain, McGlynn, and McHenry have plausibly pleaded that they have standing to bring their UCL injunction claim. Plaintiffs Duke and Page, however, have not, though the Court cannot conclude they would be unable to cure this deficiency in an amended complaint. Accordingly, the Court GRANTS Adobe's Motion to Dismiss Plaintiffs' UCL injunction claim as to Plaintiffs Duke and Page without prejudice. As to the remaining Plaintiffs, Adobe is not entitled to dismissal of Plaintiffs' UCL injunction claim on the basis of standing.

2. Contract Remedy

Adobe additionally argues that Plaintiffs' UCL injunction claim, like Plaintiffs' declaratory relief claim, is actually a contract claim in disguise. Mot. at 17. Specifically, Adobe claims that the UCL injunction claim is, in reality, a claim for specific performance of the Agreement. *Id.* ("Plaintiffs' claim ... is that Adobe should be ordered to 'honor the terms of its contracts'.... Thus, what Plaintiffs seek is the contract remedy of *specific performance.*"(quoting Compl. ¶ 129)). As specific performance is a contract remedy, Adobe contends that Plaintiffs need to plead a breach of contract claim in order to seek specific performance. *Id.* (citing *Forever 21, Inc. v. Nat'l Stores Inc.,* No. 12–10807, 2014 WL 722030, at *5 (C.D.Cal. Feb. 24, 2014); *Guidiville Rancheria of Cal. v. United States,* ––– F.Supp.2d ––––, 2013 WL 6512788, at * 13 (N.D. Cal. Dec 12, 2013)). Plaintiffs have not done so, and thus Adobe contends that Plaintiffs' UCL injunction claim fails as a matter of law. *Id.*

Plaintiffs acknowledge that they have not pleaded a breach of contract claim. Opp'n at 21. Nevertheless, Plaintiffs contend that their request for an injunction is just that–a request for an injunction under the UCL, not one for the contract remedy of specific performance. *Id.* As Plaintiffs are not seeking a contract remedy, Plaintiffs contend they do not need to plead the elements of breach of contract. *Id.*

The Court agrees with Plaintiffs that their request is indeed a request for an injunction under the UCL, and not one for specific performance. Plaintiffs do not allege that Adobe violated the UCL solely on the grounds that Adobe failed to "honor the terms of its contracts." *See* Compl. ¶¶ 128–13 1. While Plaintiffs do allege "systematic breach of [ ] contracts" as one of Adobe's allegedly unlawful practices, Plaintiffs also allege that Adobe's actions are independently unlawful because they violate the duty California imposes on businesses to reasonably safeguard customers' data under the CRA. Compl. ¶ 130; *accord* Opp'n at 21 ("Adobe's duties arose from promises it made in its contracts and elsewhere, *and from statute.*"(emphasis added)). The Court has already determined that Plaintiffs have standing to bring claims under this statute. *See supra* Part III.A. Thus, contrary to Adobe's assertion, Plaintiffs have alleged a basis for a UCL violation other than breach of contract. The Court therefore concludes that Plaintiffs' request is for an injunction to remedy Adobe's alleged UCL violations, and not to remedy an unalleged breach of contract.

3. Unlawful or Unfair

***17** Adobe further challenges Plaintiffs' UCL injunction claim on the ground that Plaintiffs do not plead any "unlawful" or "unfair" conduct that violates the UCL. Mot.

at 18–19. The Court first considers Plaintiffs' "unlawful" allegations, then turns to Plaintiffs' "unfair" allegations.

a. Unlawful

The "unlawful" prong of the UCL prohibits "anything that can properly be called a business practice and that at the same time is forbidden by law." *Cel–Tech,* 20 Cal.4th at 180 (internal quotation marks omitted). By proscribing "any unlawful" business practice, the UCL permits injured consumers to "borrow" violations of other laws and treat them as unlawful competition that is independently actionable. *Id.* As predicates for their claim under the UCL's "unlawful" prong, Plaintiffs allege that Adobe: (1) violated the CRA, (2) systematically breached contracts, and (3) "failed to comport with a reasonable standard of care and California public policy" as embodied in a number of California statutes. Compl. ¶ 130 (citing the CRA, the Online Privacy Protection Act ("OPPA"), Cal. Bus. & Prof.Code § 22576, and the Information Practices Act ("IPA"), Cal. Civ.Code §§ 1798 *et seq.*).

Adobe argues that none of these allegations are adequate to sustain a UCL claim. As to Plaintiffs' CRA allegation, Adobe contends that because Plaintiffs lack standing to bring a CRA claim, Plaintiffs similarly lack standing to pursue a UCL claim premised on a violation of the CRA. Mot. at 18. However, the Court has found that Plaintiffs *do* have standing to bring their CRA claim, and thus standing presents no barrier to Plaintiffs' efforts to base their UCL unlawful claim on Adobe's alleged violation of the CRA. Accordingly, the Court finds that Plaintiffs have adequately alleged unlawful conduct that may serve as a basis for a claim under the UCL's unlawful prong, and Adobe is therefore not entitled to dismissal of the UCL unlawful claim on this basis. Because Adobe's alleged CRA violation is sufficient to sustain Plaintiffs' UCL unlawful claim, the Court need not address Adobe's arguments concerning Plaintiffs' additional allegations of unlawful conduct.

b. Unfair

The "unfair" prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by some other law. *Korea Supply Co. v. Lockheed Martin Corp.,* 29 Cal.4th 1134, 1143 (2003). "The UCL does not define the term 'unfair.' ...[And] the proper definition of 'unfair' conduct against consumers 'is currently in flux' among California courts." *Davis v. HSBC Bank Nev., N.A.,* 691 F.3d 1152, 1169 (9th Cir.2012) (citing *Lozano,* 504 F.3d at 735). Nevertheless, there are at least two possible tests: (1) the "tethering test," which requires "that the public policy which is a predicate to a consumer unfair competition action under the 'unfair' prong of the UCL must be tethered to specific constitutional, statutory, or regulatory provisions," and (2) the "balancing test," which examines whether the challenged business practice is "immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers and requires the court to weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim." [12] *Drum v. San Fernando Valley Bar Ass'n,* 182 Cal.App. 4th 247, 257 (2010). As predicates for their claim under the UCL's "unfair" prong, Plaintiffs allege that Adobe's conduct fails the "balancing test" because the conduct was "immoral, unethical, ... or substantially injurious" and caused harm that outweighed the conduct's utility. Compl. ¶ 13 1. Plaintiffs further allege that Adobe's conduct fails the "tethering test" because the conduct violated public policy as embodied in the CRA, the OPPA, and the IPA. *Id.*

***18** Adobe contends that Plaintiffs' claim under the "balancing test" is "conclusory and formulaic." Mot. at 19. Specifically, Adobe claims that Plaintiffs do not allege any injuries stemming from Adobe's allegedly unfair conduct and thus that there is no "harm" to balance against any "utility." Reply at 9–10. As to the "tethering test," Adobe contends that Plaintiffs' allegations fail because Plaintiffs do not allege any violations of the OPPA or the IPA, Mot. at 19, or any effects that are "comparable to ... a violation of" those statutes, Reply at 9 (quoting *CelTech,* 20 Cal.4th at 187).

Adobe's argument that Plaintiffs' "balancing test" allegations are insufficient is unpersuasive. Adobe appears to object that Plaintiffs do not allege any injuries resulting from Adobe's allegedly unfair conduct in the precise paragraph of the Complaint asserting a claim under the "balancing test." Mot. at 19. However, while Plaintiffs are required to plead enough facts in support of their claims, the pleading standard is not so rigid as to insist that each count repeat every factual allegation. Rather, the complaint must be specific and clear enough *as a whole* such that the Court can evaluate the plausibility of each claim and the defendant is placed on notice as to the basis for the plaintiff's claims. *See, e.g.,Mc Vicar v. Goodman Global, Inc.,* ––– F.Supp.2d ––––, 2014 WL 794585, at *7 (C.D.Cal. Feb. 25, 2014) ("[T]he thrust

of [defendant's] argument is simply to point out that under the section entitled 'Count One: Violation of [the UCL],' the [plaintiffs] do not specifically reference the other sections of the Complaint that identify unlawful business practices.... The UCL does not create such a formalistic pleading requirement."). Elsewhere in the Complaint, Plaintiffs allege that Adobe's conduct placed Plaintiffs at a substantial risk of future harm and caused Plaintiffs to overpay for Adobe products and services. *See, e.g.,* Compl. ¶¶ 67–73, 139. The Court has already found that these allegations of injury are sufficient for Plaintiffs to have standing to bring their UCL injunction claim. *See supra* Part III. C.1. For the same reasons, the Court finds that Plaintiffs have set forth enough factual allegations of injury to bring a claim under the "balancing test."

Turning to the "tethering test," the Court notes that contrary to Adobe's assertion, Plaintiffs do not need to plead any direct violations of a statute to bring a claim under the UCL's unfair prong. Instead, Plaintiffs need merely to show that the effects of Adobe's conduct "are comparable to or the same as a violation of the law, or otherwise significantly threaten[ ] or harm [ ] competition." *Cel–Tech,* 20 Cal.4th at 187. Plaintiffs argue that the OPPA, the IPA, and the CRA collectively reflect California's public policy of "protecting customer data." Opp'n at 20. The Court agrees that California legislative intent is clear on this point, and thus finds that Plaintiffs have adequately alleged that Adobe's conduct is "comparable" to a violation of law. *See, e.g.,*Cal. Civ.Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ.Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof.Code § 22578 (explaining that the Legislature's intent was to have a uniform policy state-wide regarding privacy policies on the Internet). Accordingly, the Court concludes that Plaintiffs have pleaded adequate facts to bring a claim under the "tethering test" of the UCL's "unfair" prong.

***19** In sum, the Court concludes that Plaintiffs Duke and Page have not adequately pleaded that they have standing to bring a claim under the UCL. The Court therefore GRANTS Adobe's Motion to Dismiss this claim as to Plaintiffs Duke and Page without prejudice. However, the Court finds that Plaintiffs Halpain, McGlynn, Kar, and McHenry have adequately pleaded both standing and the necessary elements to bring their UCL injunction claim. Accordingly, the Court DENIES Adobe's Motion to Dismiss this claim as to those Plaintiffs.

D. UCL Restitution Claim

Plaintiffs' fourth and final cause of action is for restitution under the UCL on behalf of purchasers of Adobe's ColdFusion and Creative Cloud products and services ("UCL restitution claim"). *See* Compl. ¶¶ 133–140. Plaintiffs assert claims under both the "fraudulent" and "unfair" prongs of the UCL on the basis that Adobe "fail[ed] to disclose that it does not enlist industry standard security practices." Compl. ¶ 135. Adobe objects to Plaintiffs' UCL restitution claim on three grounds. First, Adobe contends that the proposed representatives of a restitution class, Plaintiffs Halpain and McGlynn, lack standing to represent ColdFusion customers as both allege only that they subscribed to Creative Cloud. Mot. at 20. Second, Adobe contends that Plaintiffs have not adequately pleaded an omission under the "fraudulent" prong of the UCL. *Id.* Third, Adobe contends that Plaintiffs have not adequately pleaded a claim under the "unfair" prong of the UCL. *Id.* at 25.

1. Standing to Bring Restitution Claims for ColdFusion Customers

Some courts reserve the question of whether plaintiffs may assert claims based on products they did not buy until ruling on a motion for class certification. *See, e.g.,Forcellati v. Hyland's, Inc.,* 876 F.Supp.2d 1155, 1161 (C.D.Cal.2012); *Cardenas v. NBTY, Inc.,* 870 F.Supp.2d 984, 992 (E.D.Cal.2012). Others "hold that a plaintiff may have standing to assert claims for unnamed class members based on products he or she did not purchase so long as the products and alleged misrepresentations are substantially similar." *Miller v. Ghirardelli Chocolate Co.,* 912 F.Supp.2d 861, 869 (N.D.Cal.2012) (citing cases); *see also, e.g.,Colucci v. ZonePerfect Nutrition Co.,* No. 12–2907, 2012 WL 6737800, at *4 (N.D.Cal. Dec. 28, 2012); *Astiana v. Dreyer's Grand Ice Cream, Inc.,* No. 11–2910, 2012 WL 2990766, at *11–13 (N.D.Cal. July 20, 2012). Still other courts have dismissed claims for lack of standing when the plaintiff did not purchase the product on which the claim is based. *See, e.g.,Granfield v. NVIDIA Corp.,* No. 11–5403, 2012 WL 2847575, at *6 (N.D.Cal. July 11, 2012) ("[W]hen a plaintiff asserts claims based both on products that she purchased and products that she did not purchase, claims relating to products not

purchased must be dismissed for lack of standing."); *Carrea v. Dreyer's Grand Ice Cream, Inc.*, No. 10–1044, 2011 WL 159380, at *3 (N.D.Cal. Jan. 10, 2011), *aff'd on other grounds*, 475 F. App'x 113 (9th Cir.2012).

This Court has previously applied the "substantially similar" approach and will do so again here. *E.g., Werdebaugh v. Blue Diamond Growers*, No. 12–2724, 2013 WL 5487236, at *12 (N.D.Cal. Oct. 2, 2013); *Brazil v. Dole Food Co.*, No. 12–1831, 2013 WL 5312418, at *7 (N.D. Cal. Sep 23, 2013). Under this approach, both the products themselves and the misrepresentations the plaintiff challenges must be similar, though not identical. In this case, the misrepresentations and omissions at issue are the same for both ColdFusion and Creative Cloud, as all Adobe products are governed by the same privacy policy. *See* Compl. ¶¶ 29–32. Adobe contends, however, that ColdFusion and Creative Cloud are sufficiently dissimilar *as products* that Plaintiffs lack standing to assert claims as to ColdFusion. Drawing from the Complaint, Adobe identifies the following differences between the two products: (1) ColdFusion is licensed-based whereas Creative Cloud is subscription-based; (2) customers use ColdFusion to build dynamic web sites whereas Adobe uses Creative Cloud to sell software subscriptions; and (3) ColdFusion costs up to several thousand dollars per license whereas Creative Cloud plans cost "between $19.99 and $79.99" a month. Mot. at 20 n. 1 1 (citing Compl. ¶¶ 19–20). The Court notes, however, that Plaintiff Halpain alleges that she uses Creative Cloud to build websites, Compl. ¶ 89, thus suggesting that both Creative Cloud and ColdFusion can be used for website development. Therefore, assuming the Complaint's allegations are true, as the Court must on a motion to dismiss, the Court is not persuaded by Adobe's second-identified difference.

***20** The Court finds that the remaining two differences between ColdFusion and Creative Cloud are not significant enough to prevent the products from being "substantially similar" for purposes of the claims alleged here. Plaintiffs' theory of harm for their UCL restitution claim is that ColdFusion and Creative Cloud are "heavily security-dependent" products that Plaintiffs either would not have purchased or for which Plaintiffs would not have paid as much had Plaintiffs known the truth about Adobe's inadequate security practices. Opp'n at 17; Compl. ¶¶ 136–139. Neither the cost of a product nor whether the product is license- or subscription-based is relevant to the inquiry here, *i.e.*, whether purchasers of the products valued security, and thus whether they overpaid for their Adobe products in light of Adobe's alleged misrepresentations and omissions regarding security. This distinguishes this case from cases applying the substantially similar approach in the food mislabeling context, where differences in the products could be expected to have an impact on whether the customer purchased the product in reliance on the defendant's misrepresentations. *See, e.g., Larsen v. Trader Joe's Co.*, No. 11–5188, 2012 WL 5458396, at *1, 4 (N.D. Cal. June 14, 2012) (plaintiffs lacked standing to challenge label statements on products plaintiffs did not purchase where products at issue were as disparate as cinnamon rolls, ricotta cheese, apple juice, and sandwich cookies). Accordingly, the Court concludes that Plaintiffs have pleaded sufficient facts to establish that Plaintiffs Halpain and McGlynn, the proposed representatives of a restitution class, have standing to assert claims related to both Creative Cloud and ColdFusion.

2. Fraudulent

For an omission to be actionable under the UCL, "the omission must be contrary to a representation actually made by the defendant, or an omission of a fact the defendant was obliged to disclose." *Daugherty v. Am. Honda Motor Co.*, 144 Cal.App. 4th 824, 835 (2006); *see also Berryman v. Merit Prop. Mgmt., Inc.*, 152 Cal.App. 4th 1544, 1557 (2007) ("[A] failure to disclose a fact one has no affirmative duty to disclose is [not] 'likely to deceive' anyone within the meaning of the UCL."(quoting *Daugherty*, 144 Cal.App. 4th at 838)). The California Courts of Appeal have held that there are four circumstances in which a duty to disclose may arise: "(1) when the defendant is the plaintiff's fiduciary; (2) when the defendant has exclusive knowledge of material facts not known or reasonably accessible to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; [or] (4) when the defendant makes partial representations that are misleading because some other material fact has not been disclosed." *Collins v. eMachines, Inc.*, 202 Cal.App. 4th 249, 255 (2011). "[A] fact is deemed 'material,' and obligates an exclusively knowledgeable defendant to disclose it, if a 'reasonable [consumer]' would deem it important in determining how to act in the transaction at issue." *Id.* at 256 (citing *Engalla v. Permanente Med. Grp., Inc.*, 15 Cal.4th 951, 977 (1997)). Plaintiffs claim that Adobe had exclusive knowledge of the fact that its security practices fell short of industry standards, and that this fact was material. Opp'n at 17–18. Accordingly, Plaintiffs claim that Adobe had a duty to disclose this fact, and that Adobe's failure to do so is an actionable omission under the UCL. *Id.*

Adobe does not dispute that facts regarding its security practices are material. Rather, Adobe contends that Adobe did not have exclusive knowledge of its security practices because Adobe's security shortcomings were widely reported in the press before the 2013 data breach. Mot. at 21–22; Reply at 11–13. Specifically, Adobe notes that its security problems were detailed in articles published by *CNN Money,* the *New York Times,* the *Wall Street Journal,* and *Reuters,* Reply at 12, and further that Plaintiffs knew of these reports, *id.*(noting that the original individual complaints cite some of these reports); *see* Compl. ¶¶ 42–46 (listing security problems prior to the 2013 data breach under the heading "Adobe's Abysmal Security Record"). Adobe notes that courts in other cases have found that defendants did not have "exclusive knowledge" of the alleged omission when the allegedly omitted fact was widely reported in similarly reputable news sources. Reply at 11–12 (citing *Herron v. Best Buy Co.,* 924 F.Supp.2d 1161, 1175–76 (E.D.Cal.2013) (finding that defendants did not have exclusive knowledge of battery testing conditions when those conditions had been reported in *Newsweek*); *Gray v. Toyota Motor Sales, U.S.A.,* No. 08–1690, 2012 WL 313703, at *8 (C.D.Cal. Jan. 23, 2012) (finding that defendant did not have exclusive knowledge of discrepancy between EPA estimate of car's gas mileage and real-world results when discrepancy was reported in *Consumer Reports* and *USA Today*)). Adobe contends that "as a matter of law and logic," Adobe could not have exclusive knowledge of the fact that it "had not implemented several industry-standard security measures." *Id.* at 11 (internal quotation marks omitted).

***21** The Court is not convinced. It is one thing to have a poor reputation for security in general, but that does not mean that Adobe's specific security shortcomings were widely known. None of the press reports Adobe identifies discusses any specific security deficiencies, and Plaintiffs expressly allege that the extent of Adobe's security shortcomings were revealed only *after* the 2013 data breach. Compl. ¶ 59. Given that prior reports of Adobe's security problems were highly generic, the Court cannot say that Adobe did not have exclusive knowledge of its failure to implement industry-standard security measures. [13] Furthermore, the exact nature of what was in the public domain regarding Adobe's security practices is a question of fact not properly resolved on a motion to dismiss.

Adobe further argues that even if Plaintiffs identify an actionable omission, Plaintiffs cannot allege that they relied on that omission, as is required for a claim under the "fraudulent" prong of the UCL. Mot. at 23 (citing *In re Facebook PPC Adver. Litig.,* No. 09–3043, 2010 WL 3341062, at *9 (N.D.Cal. Aug. 25, 2010)). Adobe reasons that both Halpain and McGlynn could have cancelled their subscriptions to Creative Cloud upon learning of Adobe's security deficiencies. Mot. at 24. Neither did so, and indeed, Halpain re-subscribed to Creative Cloud after her subscription had terminated. *Id.* Adobe argues that Plaintiffs' actions are therefore inconsistent with their allegations that they would not have subscribed to Creative Cloud had they known of Adobe's security deficiencies. *Id.* (citing *Noll v. eBay, Inc.,* No, 11–4585, 2013 WL 2384250, at *4 (N.D.Cal. May 30, 2013)).

The Court disagrees. Plaintiffs allege that they would not have subscribed to Creative Cloud in the first instance had they known of Adobe's allegedly unsound security practices. Compl. ¶¶ 84, 91. Having invested time, money, and energy in Creative Cloud, however, Plaintiffs allege that the costs to switch to another product–which include early cancellation fees, *id.* ¶¶ 88, 93–are now too high to justify abandoning their Creative Cloud subscriptions. *See* Opp'n at 19 (citing Compl. ¶ 137). This is a plausible allegation. Moreover, a plaintiff need not allege that a product became totally worthless to her once the defendant's misrepresentation came to light in order to plead actionable reliance. Rather, it is enough to allege that the product is worth *less* to the plaintiff in light of the misrepresentation. *See Kwikset,* 51 Cal.4th at 330 (plaintiff may establish reliance by alleging that she "paid more than ... she actually valued the product"). Thus, Plaintiffs need not have concluded that Creative Cloud is completely worthless, and thus have canceled their subscriptions, in order to have detrimentally relied on Adobe's alleged misrepresentations or omissions regarding security. [14] Accordingly, the Court finds that Plaintiffs have not pleaded themselves out of court by alleging that they did not cancel their Creative Cloud subscriptions upon learning of Adobe's omissions regarding security.

***22** For these reasons, the Court concludes that Plaintiffs have adequately pleaded that Adobe had a duty to disclose that its security practices were not up to industry standards, that this omission was material, and that Plaintiffs relied on this omission to their detriment. Thus, Plaintiffs have adequately pleaded their UCL restitution claim under the UCL's "fraudulent" prong, and Adobe is not entitled to dismissal of this claim.

3. Unfair

Plaintiffs also assert two claims under the UCL's "unfair" prong for their UCL restitution claim. First, Plaintiffs allege that Adobe's competition invested in industry-standard security practices, and therefore Adobe gained an unfair competitive advantage to the extent that Adobe did not. Compl. ¶ 138. Plaintiffs contend that this conduct was "unethical, unscrupulous, and substantially injurious." *Id.* Second, Plaintiffs allege that Adobe's conduct undermined California public policy as embodied in the OPPA, the IPA, and the CRA. *Id.*

Adobe's objection to these claims again is that Plaintiffs did not include all of the factual allegations supporting these claims in the section of the Complaint that lays out the UCL restitution claim. *See* Mot. at 25; Reply at 15. As previously discussed, *see supra* Part III.C.3.b., the pleading standard does not require that every factual allegation needs to be repeated for every cause of action, *e.g. Mc Vicar,* 2014 WL 794585, at *7. Elsewhere in the Complaint, Plaintiffs identify a number of specific industry-standard security measures that Adobe allegedly did not implement, Compl. ¶ 62, and allege that Adobe's competitors did invest in these measures, *id.* ¶ 138; *see also id.* ¶ 60 ("[C]ompanies like Adobe that do business with major financial institutions or credit card issues must certify that their security measures and protocols are compliant with [an industry standard]."). Plaintiffs therefore plausibly allege that Adobe gained an unfair competitive advantage by not spending money on security the way its competitors did. Plaintiffs also plausibly allege that they were injured by Adobe's conduct in that they overpaid for Adobe products as a result. *Id.* ¶ 139.

Adobe also repeats the argument that Plaintiffs' "public policy" allegations are flawed because Plaintiffs do not plead violations of the OPPA, the IPA, and the CRA. Mot. at 25. As previously discussed, *see supra* Part III.C.3.b, the "unfair" prong does not require Plaintiffs to plead direct violations of these statutes. Instead, the Court has already found that Plaintiffs plausibly allege that the OPPA, the IPA, and the CRA reflect California's policy objective of reasonably securing customer data. *See supra* Part III.C.3.b. Plaintiffs further plausibly allege that Adobe's purported failure to provide industry-standard security undermines that policy objective. The Court therefore finds that Plaintiffs have pleaded with sufficient specificity all the necessary elements of a claim under the UCL's "unfair" prong for their UCL restitution claim, and Adobe is not entitled to dismissal of the claim on that basis.

For the foregoing reasons, the Court DENIES Adobe's Motion to Dismiss Plaintiffs' UCL restitution claim.

IV. CONCLUSION

For the reasons discussed above, the Court:

1. GRANTS Adobe's Motion to Dismiss Plaintiffs' CRA claim for violations of Section 1798.82 without prejudice;

2. GRANTS Adobe's Motion to Dismiss Plaintiffs' UCL injunction claim as to Plaintiffs Duke and Page without prejudice; and

***23** 3. DENIES the remainder of Adobe's Motion to Dismiss.

Should Plaintiffs elect to file a Second Amended Complaint curing the deficiencies identified herein, Plaintiffs shall do so within thirty days of the date of this Order. Failure to meet the thirty-day deadline to file an amended complaint or failure to cure the deficiencies identified in this Order will result in a dismissal with prejudice. Plaintiffs may not add new causes of actions or parties without leave of the Court or stipulation of the parties pursuant to Federal Rule of Civil Procedure 15.

IT IS SO ORDERED.

Footnotes

1 Unless otherwise noted, all remaining ECF citations refer to Case Number 13–CV–5226.

2 Although a district court generally may not consider any material beyond the pleadings in deciding a Rule 12(b)(6) motion, the Court may take judicial notice of documents referenced in the complaint, as well as matters in the public record, without converting a motion to dismiss into one for summary judgment. *See Lee v. City of L.A.,* 250 F.3d 668, 688–89 (9th Cir.2001). A matter may be judicially noticed if it is either "generally known within the trial court's territorial jurisdiction," or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed.R.Evid. 201(b).

Here, Adobe requests that the Court take judicial notice of the transcript of the case management conference hearing held before this Court on March 13, 2014. Def. May 21 RJN Ex. A. This transcript is an appropriate subject for judicial notice, as it is a

matter of public record. Adobe also requests that the Court take judicial notice of Adobe's Privacy Policies of May 7, 2012 and December 20, 2013, *id.* Exs. B, C; Adobe's General Terms of Use, *id.* Ex. D; and the subscription terms for Adobe's Creative Cloud, *id.* Ex. E. These documents are referenced and quoted in the Complaint, *e.g.,* Compl. ¶¶ 5, 29, 30–32, 84, 91, 99, 119–120, 129, and the Court may therefore take judicial notice of these documents under the doctrine of incorporation by reference. *See, e.g.,Knievel v. ESPN,* 393 F.3d 1068, 1076 (9th Cir.2005) (district court may consider "documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the [plaintiff's] pleading" (alteration in original) (internal quotation marks omitted)). Finally, Adobe requests that the Court take judicial notice of three newspaper articles discussing Adobe's security problems. Def. July 2 RJN Exs. A, B, C. The Court may take judicial notice of the existence of these reports as indication of what was in the public realm, but not for the veracity of any arguments or facts contained within. *See Von Saher v. Norton Simon Museum of Art at Pasadena,* 592 F.3d. 954, 960 (9th Cir.2010). Accordingly, the Court GRANTS Adobe's Requests for Judicial Notice dated May 21, 2014 and July 2, 2014.

Plaintiffs request that the Court take judicial notice of one of Adobe's End User License Agreements ("EULA"). Pl. RJN Ex. A. The EULA is referenced in the Complaint, *see, e.g.,* Compl. ¶¶ 29–32, 41, 105, and is publicly available on Adobe's website. Accordingly, the Court GRANTS Plaintiffs' Request for Judicial Notice. *See Knievel,* 393 F.3d at 1076.

3 Adobe refers to Sections 1798.81.5 and 1798.82 as the "California Data Breach Notification Act," *see* Mot. at 6, whereas Plaintiffs refer to those sections as the "California Customer Records Act," *see* Opp'n at 6. The Court agrees with Plaintiffs that Section 1798.81.5 deals with more than notification in the event of a breach. *See*Cal. Civ.Code § 1798.81.5(d) ("[T]he purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information."). Accordingly, the Court will refer to these sections as the Customer Records Act ("CRA"), after the name of the Title under which they appear. *See* Cal. Civ.Code tit. 1.81 ("Customer Records").

4 Indeed, the "certainly impending" language can be traced back to a 1923 decision, *Pennsylvania v. West Virginia,* 262 U.S. 553, 593 (1923), and has been cited numerous times in U.S. Supreme Court cases addressing standing in the intervening decades. *See, e.g.,Lujan,* 504 U.S. at 564 n.2; *Whitmore,* 495 U.S. at 158; *Babbitt,* 442 U.S. at 298.

5 The Court further notes that requiring Plaintiffs to wait for the threatened harm to materialize in order to sue would pose a standing problem of its own, because the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not "fairly traceable" to the defendant's data breach. Indeed, Adobe makes this very argument in its Motion. Specifically, Adobe speculates that Plaintiff Halpain may also have been a victim of recent data breaches involving Target and Neiman Marcus, and thus that Halpain's allegation that her personal data appeared on "black market websites" is not fairly traceable to Adobe's 2013 data breach. Mot. at 9 & n.8. This argument fails, given that there is no factual basis for Adobe's speculation that Halpain was a customer of either Target or Neiman Marcus, let alone that Halpain's personal data was compromised in data breaches involving these companies.

6 It is also worth noting that *Clapper* was decided on summary judgment, *see* 133 S.Ct. at 1146, which requires that a plaintiff come forward with a greater degree of evidentiary proof to support her standing allegations than is required at the motion to dismiss stage, *see Lujan,* 504 U.S. at 561.

7 The precise degree of imminence required is somewhat uncertain. While a "certainly impending" risk of future harm would undoubtedly be sufficiently imminent to confer standing on a plaintiff who took costly measures to mitigate that risk, *Clapper* did not overrule prior cases that have found standing where a plaintiff incurs costs in order to mitigate a risk of harm that is "substantial." 133 S. Ct. at 1150 n.5 (there can be standing "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm"). The *Clapper* Court declined, however, to determine whether a "substantial" risk of future harm is meaningfully different from a "certainly impending" risk of future harm. *See id.* ("But to the extent that the 'substantial risk' standard is relevant and is distinct from the 'clearly impending' requirement, respondents fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm here."). This Court need not resolve whether there is any practical difference between the two formulations either, as the Court finds that Plaintiffs' allegations meet the "certainly impending" standard.

8 Plaintiffs additionally allege that they suffered economic injury in the form of lost value, both because the software Plaintiffs paid for is now "highly vulnerable to attacks," and because Plaintiffs Halpain and McGlynn would not have subscribed to Creative Cloud had they known of Adobe's substandard security practices. *See* Opp'n at 10. As the Court has already found that all Plaintiffs have Article III standing to pursue their CRA claims based on an increased risk of harm and, in the case of Plaintiffs Halpain and Kar, costs incurred to mitigate that risk of harm, the Court need not address this additional theory of standing.

9 *Compare*28 U.S.C. § 2201 ("In a case of actual controversy within its jurisdiction ... any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought."), *with*Cal.Civ.Proc.Code § 1060 ("Any person interested under a written instrument ... or under a contract ... may, in cases of actual controversy relating to the legal rights and duties of the respective parties, bring an

original action ... for a declaration of his or her rights and duties.... [T]he court may make a binding declaration of these rights or duties, whether or not further relief is or could be claimed at the time.").

10 Adobe contends that Plaintiffs do not allege "any adverse consequences of sufficient immediacy and reality [ ] in the absence of their requested judicial declarations." Mot. at 14 (emphasis removed). However, Plaintiffs' complaint specifically alleges that "Adobe's customers will remain at risk of attack until the company completely revamps its security practices." Compl. ¶ 66. Plaintiffs then substantiate this allegation of threatened harm by listing a number of Adobe's allegedly unreasonable security practices, *id.* ¶ 62, and identifying previous instances in which Adobe has allegedly inadequately responded to security threats, *id.* ¶¶ 43, 55.

11 Adobe resists this conclusion on the grounds that the remedial security measures Plaintiffs propose do not take into account the evolving meaning of "reasonable" and are not sufficiently specific or definitive because they refer to "industry standards" and similar undefined terms. Reply at 6. This is unpersuasive. For one thing, the Court is not bound to adopt the precise wording of any potential declaration set forth in a plaintiff's complaint in deciding how to award declaratory relief, and in any event, Adobe's objections would not prevent the Court from declaring that Adobe's current security practices are unreasonable. Such a decree would constitute "specific relief" that would conclusively address the real dispute surrounding the scope of Adobe's existing contractual obligations.

12 In *Williamson v. Reinalt–Thomas Corp.*, No. 11–3548, 2012 WL 1438812, at *11 (N.D.Cal. Apr. 25, 2012), this Court recognized that the "balancing test" is sometimes construed as two separate tests. In *Williamson,* this Court noted that some California appellate courts have interpreted the balancing test to require only that a court "weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim." *S. Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72 Cal.App. 4th 861, 886 (1999). On the other hand, other appellate state courts have applied a slightly different version of the balancing test, which mandates that plaintiffs show that a practice is "immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers." *Bardin v. Daimlerchrysler Corp.*, 136 Cal.App. 4th 1255, 1260 (2006)).

13 Adobe's reliance on *Herron* and *Gray* is misplaced. In both those cases, the press had widely reported the *exact* omission for which the plaintiffs sought to hold the defendant liable. *See Herron,* 924 F.Supp.2d at 1175–76 (no actionable omission where both the defendant and the press had reported the testing conditions used to measure a laptop's battery life); *Gray,* 2012 WL 313703, at *8 (no actionable omission where press reported that the EPA's gas mileage estimates for the Toyota Prius were significantly higher than real-world experience). There is no such specificity here.

14 Adobe's authority is not to the contrary. In *Noll,* the plaintiffs alleged that defendant eBay failed to disclose that listing fees automatically recurred every 30 days. 2013 WL 2384250, at *2. Critically, the *Noll* plaintiffs did not allege that they would incur any costs, direct or hidden, if they cancelled their listings. *Id.* Yet the *Noll* plaintiffs continued to pay the listing fees even after they discovered that the fees recurred automatically. *Id.* Their behavior after discovering the omission was therefore exactly the same as their behavior before they knew of the omission, logically foreclosing any allegations of reliance. *Id.* at *4. Here, in contrast, Plaintiffs plausibly allege that they faced costs to cancelling their subscriptions and to not re-subscribing that they did not face when deciding whether to subscribe to Creative Cloud in the first place.

End of Document

Exhibit “B”

MM-T

IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ERICA TIERNEY, et al.,	)	
	)	
	)	
Plaintiffs,	)	Civil Action No. 13 CV 6237
	)	
v.	)	Hon. Charles R. Norgle
	)	
ADVOCATE HEALTH AND HOSPITALS CORPORATION,	)	
	)	
	)	
Defendant.	)	

ORDER

Advocate Medical Group's Motion to Dismiss [56] is granted in part. The Court dismisses Counts I and II with prejudice. Because no federal claims remain in the case, in its discretion, the Court relinquishes jurisdiction over the state-law claims. As the prevailing party, Defendant is admonished to comply with Federal Rule of Civil Procedure 54(d)(1) in submitting a bill of costs, if any.

STATEMENT

In this putative class action lawsuit, Plaintiffs Erica Tierney ("Tierney"), Andris Strautins ("Strautins"), Natalie Robles ("Robles"), Jeffrey Benkler ("Benkler"), Erick D. Oliver ("Oliver"), and Lili Robins ("Robins") (collectively, "Plaintiffs") sue Defendant Advocate Health and Hospital Corporation ("Defendant") for willful and negligent violations of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.* (Counts I and II). Additionally, Plaintiffs assert state-law claims of negligence (Count III) and invasion of privacy by public disclosure of private facts (Count IV) under supplemental jurisdiction. Before the Court is Defendant's motion to dismiss Plaintiffs' Amended Class Action Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6). For the following reasons, the motion is granted in part. Counts I and II are dismissed; and, in its discretion, the Court relinquishes jurisdiction over the state-law claims.

Defendant is a network of affiliated doctors and hospitals that provides medical care to patients throughout Illinois. Defendant maintains personally identifiable information and personal health information for its own files and also submits this information to insurance companies and state and federal agencies to obtain payment for health care services provided to its patients. These files contain health information, including names, addresses, dates of birth, Social Security numbers, treating physician and/or departments for each patient, their medical diagnosis, medical record numbers, medical services codes, and health insurance information. The files do not include any information about its patients' ability to pay their medical bills. On July 15, 2013, four desktop computers which contained patient information were stolen from one

of Defendant's offices. Plaintiffs allege that Defendant improperly stored their personal information which directly and proximately caused a data breach, i.e., the theft and dissemination of private information into the public domain.

As an initial matter, the Court considers sua sponte the issue of subject matter jurisdiction. Craig v. Ontario Corp., 543 F.3d 872, 874 (7th Cir. 2008) ("Naturally, the first question [the Court] must confront is that of jurisdiction."); see also Wellness Int'l Network, Ltd. v. Sharif, 727 F.3d 751, 768 (7th Cir. 2013) ("[P]arties cannot consent to subject-matter jurisdiction; indeed, such questions must be considered by a court sua sponte." (citations omitted)). Plaintiffs—as the party invoking federal jurisdiction—bear the burden to establish standing. Scanlan v. Eisenberg, 669 F.3d 838, 841 (7th Cir. 2012). Plaintiffs must show:

> "(i) an injury in fact, which is an invasion of a legally protected interest that is concrete and particularized and, thus, actual or imminent, not conjectural or hypothetical; (ii) a causal relationship between the injury and the challenged conduct, such that the injury can be fairly traced to the challenged action of the defendant; and (iii) a likelihood that the injury will be redressed by a favorable decision."

Id. (quoting Lee v. City of Chi., 330 F.3d 456, 468 (7th Cir. 2003)). To satisfy the first requirement, an injury in fact, Plaintiffs must show that they have "sustained or [are] immediately in danger of sustaining some direct injury." Id. (internal quotation marks and citation omitted).

Here, Tierney, Strautins, Robles, and Robinson allege only a speculative fear of harm that someone could have bought and sold their personally identifiable information and personal health information on the international cyber black market and thereby place them at risk of identity theft, identity fraud, and medical fraud. Without any allegations to support their mere conclusion of imminent harm, they fail to establish standing. See Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1151 (2013) ("[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." (citations omitted)).

In contrast, Benkler and Oliver allege that they were injured insofar as each was notified of fraudulent activity—namely, that one or more individuals had attempted to access personal bank accounts and had opened cell phone accounts, respectively. Moreover, Benkler alleges that he has never been a victim of a data breach aside from Defendant's data breach. Oliver also alleges that other than the notification from Defendant regarding its data breach he has not otherwise been informed that his personal information has been compromised. Both Benkler and Oliver allege a causal relationship between their injuries and Defendant's alleged wrongful actions. Finally, Benkler and Olvier "narrate[] a claim that arises under federal law"—the FCRA. Bovee v. Broom, 732 F.3d 743, 744 (7th Cir. 2013). The relief that they seek from their alleged injuries is not too attenuated to warrant dismissal for lack of standing.

Next, the Court addresses Defendant's arguments pursuant to Rule 12(b)(6). To survive a motion to dismiss under Rule 12(b)(6), a complaint must allege "enough facts to state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). That is, Plaintiffs' Amended Class Action Complaint "must actually *suggest* that the plaintiff has a right to relief, by providing allegations that raise a right to relief above the speculative level." Indep. Trust Corp. v. Stewart Info. Servs. Corp., 665 F.3d 930, 935 (7th Cir. 2012) (internal quotation marks and citation omitted). The Court accepts as true all well-pleaded facts alleged in

Plaintiffs' Amended Class Action Complaint and draws all reasonable inferences in their favor. Killingsworth v. HSBC Bank Nevada, N.A., 507 F.3d 614, 618 (7th Cir. 2007) (citation omitted); see also Adams v. City of Indianapolis, 742 F.3d 720, 728 (7th Cir. 2014). But the Court "need not accept as true legal conclusions, or threadbare recitals of the elements of a cause of action, supported by mere conclusory statements." Alam v. Miller Brewing Co., 709 F.3d 662, 666 (7th Cir. 2013) (internal quotation marks and citation omitted). Additionally, Plaintiffs "can plead [themselves] out of court by pleading facts that show [they have] no legal claim." Atkins v. City of Chi., 631 F.3d 823, 832 (7th Cir. 2011) (citations omitted).

Defendant argues that Plaintiffs' claims under the FCRA should be dismissed because, as a matter of law, the statute does not apply to Defendant. Specifically, Defendant argues that Plaintiffs have not and cannot plausibly allege that it constitutes a consumer reporting agency within the meaning of the FCRA. The Court agrees.

Under the FCRA, a "consumer reporting agency" is:

> any person which . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C.A. § 1681a(f). Defendant—a health care provider—does not engage in such a practice. The Court rejects Plaintiffs' arguments to the contrary. "The [Fair Credit Reporting Act] does not impose obligations upon a creditor who merely passes along information concerning particular debts owed to it." Mirfasihi v. Fleet Mortg. Corp., 551 F.3d 682, 686 (7th Cir. 2008) (citing DiGianni v. Stern's, 26 F.3d 346, 349 (2d Cir. 1994)) (alteration in original). Moreover, as Defendant argues, Plaintiffs fail to plausibly allege that Defendant "furnished" any information to a third party; rather, Plaintiffs allege that computers containing personal information were stolen. See, e.g., Holmes v. Countrywide Fin. Corp., No. 5:08-CV-00205-R, 2012 WL 2873892, at *16 (W.D. Ky. July 12, 2012) (holding that "[n]o coherent understanding of the words 'furnished' or 'transmitted'" was implicated under the FCRA where the plaintiffs alleged a theft of private information). Because Plaintiffs fail to plausibly allege that Defendant is a consumer reporting agency or that it furnished any information to a third party, their claims under the FCRA are dismissed.

In its discretion, the Court relinquishes jurisdiction over Plaintiffs' remaining state-law claims. See 28 U.S.C. § 1367(c)(3); RWJ Mgmt. Co. v. BP Prods. N. Am., Inc., 672 F.3d 476, 479 (7th Cir. 2012). The Court need not address Defendant's remaining arguments.

IT IS SO ORDERED.

ENTER: Charles R. Norgle

CHARLES RONALD NORGLE, Judge
United States District Court

DATE: September 4, 2014